MASTER'S THESIS

Inzicht in Cyber risico's voor het MKB

Het ontwikkelen van een raamwerk waarmee een MKB-ondernemer inzicht krijgt in de risico's voor zijn bedrijfsvoering, vanwege onvoldoende genomen cybersecuritymaatregelen

Slaager, B.

Award date:
2021

Inzicht in Cyber risico's voor het MKB.

Het ontwikkelen van een raamwerk waarmee een MKB-ondernemer inzicht krijgt in de risico's voor zijn bedrijfsvoering, vanwege onvoldoende genomen cybersecuritymaatregelen.

Cyber risks insight for SMEs.

Developing a framework in order to address a SMEs business processes risks in comparison to taken cyber security measures.

Opleiding:	Open Universiteit, faculteit Bètawetenschappen Masteropleiding Business Process Management & IT
Programma:	Open University of the Netherlands, faculty of Science Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeertraject Business Process Management and IT
Student:	Benedikt F.L. Slaager
Datum:	16-04-2021
Afstudeerbegeleider	Prof. dr. ir. Johan Versendaal
Meelezer	Prof. dr. Rob Kusters
Versie nummer:	1.3
Status:	Concept

Abstract

Benedikt Slaager, Open University of the Netherlands, faculty of Management, Science & Technology
Abstract of Master's Thesis, Submitted October 31, 2020
Developing a Cyber security framework in order to address a SMEs business processes risks

The goal of this study was to develop a framework in order to address SMEs business processes risks in relation to taken cyber security measures. Large cooperation's spend millions on Cybersecurity and hire expensive Cybersecurity specialists to try and battle Cybercrime. But for many smaller companies and especially SME's it is still very difficult to imagine the threat of Cybercrime and to anticipate and act accordingly. SME's lack insight into Cyber risks. Therefor the main objective was to develop a self-measurement cybersecurity tool. This study was designed by first conducting a literature study into three constructs: process maturity, level of digitalization and taken Cybersecurity measures. After presenting these into a framework, interviews with Cyber specialists resulted into specific risks for the various levels which were added to the framework. Finally, this framework was judged by the specialists for usability. The results of this study show that the framework is applicable for identifying security risks and more, that most of these risks are business related instead of technology related. Further research is recommended to tailor the framework for specific SME domains of expertise to enhance the usability of the framework.

Sleutelbegrippen

Cyber security, SME, risk assessment, security scan, Cyber maturity level, Business Process risk

Samenvatting

Anno 2021 zijn digitale systemen niet meer weg te denken uit de huidige maatschappij en van cruciaal belang voor bedrijven. Onlosmakelijk heeft deze digitale revolutie ook een andere sector teweeggebracht, namelijk die van de cybercrime. Er gaat geen dag voorbij zonder dat er een bedrijf is stilgelegd door ransomware of waarbij er intellectueel eigendom is gelekt. Veel grote ondernemingen spenderen miljoenen aan cybersecurity en het inhuren van specialisten om de eigen kwetsbaarheden te ontdekken en vervolgens te kunnen mitigeren. Maar voor veel MKB'ers is dit nog steeds een vaak ontastbare dreiging en lijken de kosten niet op te wegen tegen de risico's. Het is voor het MKB heel lastig om zelfstandig inzicht te krijgen in de cyberrisico's die zij lopen ten opzichte van de maatregelen die ze genomen hebben, zonder daarvoor dure specialisten in te huren.

Het MKB heeft onvoldoende inzicht in de risico's van cybercrime, en met name de effecten ervan, voor de organisatie door het gebrek aan een waardering van zijn eigen cyberweerbaarheid. Het MKB mist een methode om de impact van de genomen maatregelen te meten aan de (nog resterende) risico's voor de bedrijfsvoering.
In dit onderzoek is gepoogd antwoord te krijgen hoe een raamwerk eruitziet waarmee een MKB-ondernemer inzichtelijk krijgt welke (effecten van) risico's hij loopt voor zijn bedrijfsvoering, vanwege onvoldoende genomen cyberweerbaarheidsmaatregelen. Hierbij is er aan de hand van drie geoperationaliseerde constructen bepaald wat de restrisico's zijn. Deze constructen zijn: procesvolwassenheid, mate van digitalisatie en genomen cyberweerbaarheidsmaatregelen.

Volwassenheidsniveau	Initial	Basic t/m Efficiency	Optimizing
Ad-Hoc	• Bedrijfscontinuïteit in gevaar • Geen indicatoren / Detectie • juridische aansprakelijkheid • Makkelijk doelwit • Onnodige kosten op termijn • Geen herstel mogelijk na incident	• Laag veiligheidsbewustzijn medewerker • Onnodige kosten • Geen indicatie op incidenten • Weerstand tegen maatregelen • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Bedrijfscontinuïteit in gevaar • Efficiëntie beperkingen • Mens als risico, door focus op IT • Gebruiksvriendelijkheid neemt af • Schijnveiligheid • Zeer hoge kosten • Cybermoeheid bij medewerkers
Engaged t/m Managed	• Afhankelijkheid van anderen stijgt • Connecties zijn onbekend • Toenemende complexiteit • Introductie van nieuwe risico's • Kennis als knelpunt • Geen herstel mogelijk na incident • Hoge kwetsbaarheid • Juridische aansprakelijkheid • IT als grootste risico	• Afhankelijkheid van anderen stijgt • Scheefgroei • Toenemende complexiteit • Kennis als knelpunt • Weerstand • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Toenemende complexiteit • Kennis als knelpunt • Afhankelijkheden stijgen • Gebruiksvriendelijkheid neemt af • Schijnveiligheid • Zeer hoge kosten • Cybermoeheid bij medewerkers
Optimized	• Afhankelijkheid van externen • Verkeerde bedrijfsdoelstellingen • Hoge overhead kosten • Schijnveiligheid • Verminderde flexibiliteit • Hoge mate van complexiteit • SPOF (Single point of Failure) • Nieuwe risico's worden geïntroduceerd • Hoge kwetsbaarheid • Juridische aansprakelijkheid • IT als grootste risico	• Afhankelijkheid van externen • Verkeerde bedrijfsdoelstellingen • Hoge overhead kosten • Verminderde flexibiliteit • Hoge mate van complexiteit • SPOF (Single point of Failure) • Nieuwe risico's worden geïntroduceerd • Weerstand bij medewerkers • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Afhankelijkheid van externen • Hoge overhead kosten • Schijnveiligheid • Hoge mate van complexiteit • Cybermoeheid bij medewerkers

Mate van volwassenheid procesinrichting en digitalisatie

Mate van genomen cyberweerbaarheidsmaatregelen

Om antwoord te kunnen geven op de onderzoeksvraag is door middel van een literatuurstudie eerst voor elk van de niveaus een graadmeter ontwikkeld op basis van reeds bekende volwassenheidsniveaus waarbij de bruikbaarheid voor het MKB centraal stond. Vervolgens is een model ontwikkeld waar, aan de hand van deze constructen, een positie uit komt. Om dit model te kunnen vullen met de risico's die een MKB'er dan nog loopt zijn er semigestructureerde interviews gehouden met specialisten uit het cybersecurity domein. Deze interviews zijn door middel van codering vertaald naar een aantal risico's per niveau en daarmee is het model gevuld. Als

validatieslag is vervolgens het gevulde model verzonden naar de respondenten voor een check op correctheid en bruikbaarheid voor het MKB.

Dit alles heeft geleid tot een model met zowel op de X- als op de Y-as een drietal niveaus waarbij op basis van de drie constructen een corresponderende locatie duidelijk wordt. Daardoor krijgt een MKB'er in een oogopslag een overzicht van de voornaamste risico's voor zijn bedrijfsvoering, vanwege onvoldoende genomen cyberweerbaarheidsmaatregelen. De verwachting was dat er meer technische risico's uit de interviews naar voren zouden komen. Echter, ondanks de diversiteit van de respondenten (van pentester t/m managementniveau), bleek herhaaldelijk dat de bedrijfsvoering risico's meer van belang zijn, en de technische aspecten een achterliggende oorzaak hebben.

Dit onderzoek heeft te allen tijde het doel gehad een model te ontwikkelen wat generiek is voor het MKB. Dit betekent dat de sector waar de MKB'er zich in bevindt buiten scope is gebleven. Het verdient dan ook de aanbeveling om voor vervolgonderzoek te kijken of er een verdiepingsslag gemaakt kan worden op het ontwikkelde model specifiek voor een bepaalde sector. Daarnaast is het principe van "weten wie je vijanden zijn" een interessant aspect dat niet is meegenomen in dit onderzoek, maar dit zou wel bepaalde keuzes kunnen beïnvloeden. Dit wordt ook specifiek beschreven in de dreigingsscenario's van het Cybersecuritybeeld Nederland van de NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid). Dit principe gaat ervan uit dat er bij het bepalen van het netto risico ook gekeken moet worden naar de waarschijnlijkheid van bepaalde bedreigingen.

Summary

In 2021 it is impossible to imagine a world were companies do not rely on digital systems in some sort. But this digital revolution also adhered to the rise of an alternate shadier business opportunity, which is called Cybercrime. Every single day the news reports about another ransomware attack which brought a business to a standstill or about a data breach which severely damages a business reputation. Large cooperation's spend millions on Cybersecurity and hire expensive Cybersecurity specialist to try and battle Cybercrime. But for many smaller companies and especially SME's it is still very difficult to imagine the threat of Cybercrime and the amount of money these specialists and security measures cost do not look like to match to the potential risk for the company. Without these specialists it is almost impossible for SME's to get insight into the remaining Cyber risks pertaining to the measures they have already taken to defend themselves.

SME's lack insight into Cyber risks (and their effects) because of the absence of a self-measurement tool for Cybersecurity. This study aims to develop a framework in order to address a SMEs business processes risks in comparison to taken Cybersecurity measures. To be able to make a sound judgement this study focused on three constructs, which are: process maturity, level of digitalization and taken Cybersecurity measures.

To be able to answer the main question how this framework would look like, we started by conduction a literature study into maturity frameworks for the three levels. The focus was to find maturity levels that were suitable for SME's. After that a framework was developed which connected the three constructs and presented a specific position on the matrix. After that it was time to complete the framework by investigating into the correlating risks for SME's. This was done by conducting semi-structured interviews with Cybersecurity specialists. The interviews have been coded and translated into specific risks per maturity level and used to complement the developed framework. Afterwards the respondents were asked to check the framework for usability by a survey to validate the discovered risks.

All in all this lead to a final framework that consists, both horizontally and vertically, of three levels. Based on the three constructs a SME's can be connected to a specific level on the framework which then gives him an overview of the remaining Cyber risks for his company. We can see then, that most of these risks adhere to the business side instead of more technical risks. This was unexpected, even so because the diversity of the respondents ranged from Penn testers tot CISO's.

This study served as an opportunity to develop a framework that is usable for every SME. That meant that the specific area where a SME is working in (IT, medical, etc.) was not taken into account when conducting the study. For future research it is strongly advised to specify the framework for certain areas to enhance the usability of the framework. Besides going into depth on the specific area of expertise it is also beneficial to know your enemies and take this into consideration for future studies. Such advice is also mentioned by the NCTS (National Coordinator on Terrorism and Security) in the Cybersecurity scope for the Netherlands.

Inhoudsopgave

1. Introductie

1.1. Achtergrond

Medio 2017 werd de wereld opgeschrikt door een uitbraak van het WannaCry virus (Jong, 2017). Dit virus zorgde ervoor dat elke computer die vatbaar was voor de kwetsbaarheden waar dit virus gebruik van maakte, werd versleuteld. Dit virus maakte direct zichtbaar dat cybercrime geen onderscheid maakt in zijn slachtoffers. Van grote multinationals tot individuele gebruikers, eenieder liep het risico te worden geïnfecteerd en daardoor zijn volledige data op het gebruikte systeem te verliezen. Daarnaast hebben de recente kwetsbaarheden in de wereldwijd bekende software Citrix (NCSC, 2020) en Microsoft Exchange (NCSC, 2021) aangetoond dat ook het niet op orde hebben van zaken als patchbeleid vernietigende gevolgen kan hebben.

Deze uitbraken zorgen ook voor grote problemen bij Nederlandse MKB'ers die niet geëquipeerd waren om hier weerstand tegen te bieden. In de provincie Limburg was dit onder andere de reden voor het oprichten van een samenwerkingsplatform om de Cyberweerbaarheid te vergroten(PVO & Brightlands, 2018). Volgens dit samenwerkingsplatform is het van belang dat het MKB zowel beter bestand is tegen, alsook inzicht krijgt in de risico's van cybercrime. Daarom wordt, als onderdeel van dit cyberweerbaarheidsproject een weerbaarheidsscan ontwikkeld. Dit onderzoek zal bijdragen aan de analyse van deze weerbaarheidsscan waaruit voor de ondernemer zichtbaar wordt wat voor impact dit kan hebben op de bedrijfsvoering. Op basis hiervan kan een ondernemer kiezen waar hij de focus om moet leggen om zijn bedrijf zo goed en efficiënt mogelijk te beschermen.

In hoofdstuk één is achtergrondinformatie en de probleemstelling gepresenteerd, waarna de aanpak in hoofdlijnen is toegelicht. In hoofdstuk twee is het literatuuronderzoek gepresenteerd en een voorlopig model ontworpen, om vervolgens in hoofdstuk drie dieper in te gaan op de methodologie van het onderzoek. In hoofdstuk vier ligt de focus op het toetsen van het model en de resultaten van het onderzoek. Uiteindelijk vindt in hoofdstuk vijf de discussie plaats. De discussie zal gebruikt worden om de conclusie te formuleren en geeft tevens aanbevelingen voor de praktijk en verder onderzoek aan.

1.2. Gebiedsverkenning

Zoals gezegd wordt in dit onderzoek ingegaan op de risico's van cybercrime en hoe MKB'ers zich daartegen kunnen wapenen. Want juist deze groep is steeds vaker slachtoffer van cybercrime (Chabinsky, 2013). In een recent internationaal onderzoek is gebleken dat grote multinationals moeite hebben om grip op cybercrime te krijgen, mede vanwege dat veel bedrijven niet intensief genoeg op zoek gaan naar de risico's in het digitale domein (Castelli, Gabriel, Yates, & Booth, 2018). Voor het MKB blijkt dit een onbegonnen zaak. Daar komt bij dat cyber security vaak wordt gezien als een overhead kostenpost en niet als een intrinsiek onderdeel van de bedrijfsvoering (Ashrafi & Kuilboer, 2001). Door middel van inzicht in de te beschermen categorieën kan de cyber weerbaarheid van deze organisaties aan het licht worden gebracht.

Cybercrime wordt de laatste jaren in toenemende mate benoemd, maar wat houdt dit nu precies in?

> De betekenis van de term cybercrime is dezelfde als die van cybercriminaliteit of computercriminaliteit. Hierbij gaat het om misdaad gepleegd met ICT, gericht op ICT. Het strafbare feit wordt dus gepleegd met een computer, smartphone, smartwatch of tablet,

> kortom alles waar een processor in zit. Voorbeelden van cybercrime zijn hacking, DDoS-aanvallen, ransomware, virussen, malware, enzovoort (Justitie, 2019).

Het Amerikaanse overheidsinstituut voor standaarden en technologie (NIST) heeft een standaard ontwikkeld voor ICT-security (Tim Grance, 2003). Hierin worden alle benodigde rollen en verantwoordelijkheden voor het inzetten van ICT binnen een onderneming beschreven. Ook worden alle aspecten benoemd die nodig zijn om ICT op een veilige manier te gebruiken. Hierbij worden bijvoorbeeld “incident handling” en “monitoring” benoemd, maar ook technische veiligheidsaspecten zoals firewalls worden beschreven. Opvolgend kwam de NIST met een handleiding voor het uitvoeren van informatie beveiligings-risico assessments (Initiative, 2012), welke gebruikt kan worden om deze risico’s voor een onderneming in kaart te brengen. Deze handleiding verdeelt een onderneming in een drietal niveaus: organisatie, bedrijfsprocessen en informatiesystemen. De Nederlandse Orde van Register EDP-Auditors heeft met gebruik van onder andere bovengenoemde standaard een Cyber Security Assessment ontwikkeld (NOREA, 2015) die het mogelijk maakt een organisatie aan de hand van zeven categorieën tegen het licht te houden.

Bovenstaande methoden en standaarden zijn ontwikkeld om ervoor te zorgen dat er een bepaalde mate van Cyber Security is. De volgende definitie van het NCSC wordt gebruikt om Cyber Security uit te leggen, te weten:

> Cyber Security is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie (Definitie NCSC, juni 2012).

Het definiëren van risico’s voor een organisatie wordt veelal gedaan volgens risico management raamwerken, zoals de ISO31000 (Purdy, 2010), en is bedoeld om een organisatie inzicht te geven op basis waarvan beslissingen genomen kunnen worden over de inzet van schaarse middelen (budget, personeel, kennis, etc.). Veelal wordt risico omschreven als een nadelig effect dat kan optreden vermenigvuldigd met de kans dat dit effect optreedt. Daarnaast kan er nog een onderscheid gemaakt worden tussen bruto en netto risico (VO-raad, 2013), waarbij bruto risico’s genomen maatregelen niet meenemen in de beoordeling en netto risico’s hier wel naar kijken. Cyber risico’s specifiek hebben geen eenduidige definitie (Strupczewski, 2021), maar kunnen wel onderverdeeld worden in drie categorieën; bron van risico, risico object en impact van risico. In dit onderzoek worden de gevolgen (oftewel impact van risico) die de grootste kans hebben om op te treden, na het in acht nemen van de genomen maatregelen, beschreven als risico’s. Dit is ook wel te beschrijven als het risico effect. Door juist het effect dat cyber risico’s op kunnen leveren in het model op te nemen wordt in een oogopslag duidelijk wat dit betekend voor een MKB organisatie. Zo is het risico van een ransomware aanval minder tastbaar voor een MKB’er dan het effect dat dit oplevert, namelijk een nadelige impact op de bedrijfscontinuïteit.

Om de juiste scope van het onderzoek te definiëren is het verder van belang de definitie MKB duidelijk te stellen. In dit onderzoek wordt de definitie van de Rijksdienst voor Ondernemend Nederland (RVO) gebruikt, te weten:

Grootte	Aantal werknemers	EN	Jaaromzet	EN/ OF	Jaarbalans
Middelgroot	minder dan 250		hoogstens € 50 miljoen		kleiner of gelijk aan € 43 miljoen
Klein	minder dan 50		hoogstens € 10 miljoen		kleiner of gelijk aan € 10 miljoen
Micro	minder dan 10		hoogstens € 2 miljoen		kleiner of gelijk aan € 2 miljoen

1.3. Probleemstelling

Uit onderzoek (Gupta & Hammond, 2005; Osborn, 2015; PVO & Brightlands, 2018) blijkt dat er weinig wetenschappelijk materiaal en aandacht is voor het bepalen van cybersecurity binnen het MKB wat betreft risico's voor de bedrijfsvoering. Veel van de beschikbare cybersecurity-criteria zijn opgesteld door cybersecurityinstellingen, maar dienen uitgevoerd te worden door security professionals, EDP-auditors of ander gespecialiseerd personeel. Veelal zijn deze criteria zeer technisch van aard en prijzig om uit te voeren. Deze zorg bestaat ook bij overheden en grote bedrijven die zaken doen met het MKB (Osborn, 2015). Dit onderzoek is erop gericht MKB'ers te voorzien van een raamwerk waarmee zij de risico's kunnen bepalen voor de bedrijfsvoering van de organisatie. De verwachting is dat zij deze risico's kunnen bepalen aan de hand van de volwassenheid van de organisatie op het gebied van bedrijfsprocessen, digitalisatie en dit af te zetten tegen de reeds genomen cyberweerbaarheidsmaatregelen. Onderzoek heeft in het verleden al deels gekeken naar het verband tussen proces en risico's voor het MKB (Lim, 2010) en tussen IT en risico's (Trim & Lee, 2016), maar nog niet in relatie tot de andere genoemde constructen. Bedrijfsprocessen worden algeheel beschouwd als een maatstaf voor het bepalen van het volwassenheidsniveau van een organisatie in het algemeen (Tarhan, Turetken, & Reijers, 2016). Tevens geeft dit een duidelijk beeld wat de belangrijkste processen voor een organisatie zijn om te functioneren en hoe deze met elkaar verbonden zijn. Zonder deze processen is er geen onderneming. Daarnaast is volwassen digitalisatie een succesbepalende factor voor de operatie van een onderneming en van cruciaal belang om competitief te blijven in de markt (De Haes & Van Grembergen, 2009; De Haes, Van Grembergen, & Debreceny, 2013; Weill & Ross, 2009). De mate van digitalisatie geeft ook een beeld van de verwevenheid en afhankelijkheid van IT in een organisatie en geeft op deze manier dus inzicht waar een organisatie vatbaar kan zijn voor cybercrime("MITRE ATT&CK MATRIX," 2020). Als derde zorgt de mate van reeds genomen maatregelen ervoor dat de bruto risico's afgezet kunnen worden tegen de genomen mitigerende maatregelen om zodoende tot een netto risico resultaat te komen. Met het in acht nemen van de genomen weerbaarheidsmaatregelen geeft een raamwerk namelijk inzicht aan een ondernemer waar deze nog keuzes kan maken om de netto risico's verder te verkleinen. Dit alles met als doel een bijdrage te kunnen leveren aan de cyberweerbaarheid van het MKB.

De probleemstelling luidt dan ook:

'Het MKB heeft onvoldoende inzicht in de risico's van cybercrime voor de organisatie door het gebrek aan een waardering van zijn eigen cyberweerbaarheid. Het MKB mist een methode om de impact van de genomen maatregelen te meten aan de (nog resterende) risico's voor de bedrijfsvoering, waarbij de bestaande volwassenheid van de bedrijfsprocessen en de mate van digitalisering een rol spelen'

1.4. Opdrachtformulering

Aan de hand van de verschillende risico's die aan het einde van dit onderzoek onderkend worden, kan een organisatie een beter beeld krijgen van haar weerbaarheid tegen cybercrime. Wanneer aan deze kennis een volwassenheidsniveau gekoppeld wordt, is het mogelijk om adviezen ter verbetering van de weerbaarheid te formuleren. Dit is van groot belang voor de beveiliging van belangrijke gegevens. Beredeneert vanuit de probleemstelling volgt de hoofdvraag voor dit onderzoek:

> *Hoe ziet een raamwerk eruit waarmee een MKB-ondernemer inzichtelijk krijgt welke risico's hij loopt voor zijn bedrijfsvoering, vanwege onvoldoende genomen cyberweerbaarheidsmaatregelen?*

Deze hoofdvraag leidt, gegeven de relatie met 1) procesvolwassenheid, 2) mate van digitalisering en 3) reeds genomen cyberweerbaarheidsmaatregelen, tot de volgende deelvragen die beantwoord worden gedurende het theoretische deel van het onderzoek:

1.1. *Welke modellen zijn er al bekend ter beoordeling van de 'mate van volwassenheid procesinrichting' en welk model kan als determinant dienen voor het MKB?*
1.2. *Welke modellen zijn er al bekend ter beoordeling van de 'mate van digitalisering' en welk model kan als determinant dienen voor het MKB?*
1.3. *Welke modellen zijn er al bekend ter beoordeling van de genomen cybersecuritymaatregelen en welk model kan als determinant dienen voor het MKB?*
1.4. *Hoe zijn de reeds bestaande modellen te synthetiseren tot een raamwerk?*

De antwoorden op deze deelvragen resulteren vervolgens in een overzicht van categorieën die gebruikt kunnen worden voor het analyseren van de cyberweerbaarheid van het MKB. Daarna zal bekeken worden hoe hier een bepaalde waarde aan gekoppeld kan worden. Dit resulteert in de onderzoeksvragen die het uitgangspunt vormen voor het empirische deel van dit onderzoek.

2.1. *Hoe is het ontwikkelde model toe te passen op een MKB-organisatie?*
2.2. *Welke risico's zijn te verbinden aan de verschillende niveaus van het ontwikkelde model?*
2.3. *Op welke manier is de validiteit van het model te meten?*

1.5. Motivatie/relevantie

Veel subcategorieën van IT hebben een volwassenheidsmodel of raamwerk om te bepalen in welk stadium een organisatie zich bevindt, bijvoorbeeld voor software (Paulk, Weber, Curtis, & Chrissis, 1995). Voor cybersecurity risico's is dit nog niet het geval, onder andere door een diversiteit van deelgebieden die hierin bestaan. Veel grote organisaties zien de relevantie van cybersecurity wel in, maar bezitten vaak niet de expertise en besteden dit uit aan specialistische bedrijven (Dhillon & Torkzadeh, 2006). Voor kleinere bedrijven of zelfstandigen is dit vaak niet betaalbaar. Daarnaast is het voor veel kleinere ondernemingen nog vaak een "ver van mijn bed show". Uit onderzoek is gebleken dat vooral kleine ondernemingen vaak ten prooi vallen aan cybercrime (Rosenberg, 2018),

maar niet weten hoe hier adequaat mee om te gaan. Het juist deze groep voorzien van een weerbaarheidsscan die zij zelf kunnen uitvoeren, is daarom van uiterst belang en hiervoor is dan ook het project cyberweerbaarheid opgezet. Dit onderzoek richt zich op het bepalen van de risico's voor de bedrijfsvoering aan de hand van de mate van ingezette cyberweerbaarheidsmaatregelen. In de wetenschappelijke literatuur is er nog weinig onderzoek gedaan naar de mogelijkheid tot meten van het cyberweerbaarheid niveau van het MKB (Gupta & Hammond, 2005). Veelal zijn onderzoeken gericht op grote organisatie (Cybenko, 2014) of op een specifieke sector zoals IoT (Internet of Things) (Industry, 2018).

1.6. Aanpak in hoofdlijnen

Dit onderzoek volgt principes van Design Science Research (Hevner, March, Park, & Ram, 2004). Deze principes zijn gekozen omdat de probleemstelling te omschrijven is als een 'wicked problem'. Dit soort complexe onderzoeken resulteren vaak in nieuwe 'artefacten', zo ook in dit onderzoek waar de gevonden resultaten en conclusies uiteindelijk resulteren in een nieuw raamwerk voor het MKB.

Hoofdstuk één beschrijft de aanleiding, de gebiedsverkenning en probleemstelling. Vervolgens zijn de hoofd- en deelvragen geformuleerd waar in dit onderzoek antwoord op gegeven zal worden.

Hoofdstuk twee geeft inzicht in het theoretisch kader van het onderzoek. In dit hoofdstuk wordt beschreven hoe de literatuurstudie is opgezet en uitgevoerd. Daarna wordt het ontwikkelde raamwerk aan de hand van de gevonden literatuur getoond en afgesloten met de relevantie van het vervolgonderzoek.

Hoofdstuk drie beschrijft de methodologie van het onderzoek. Hierna volgt de beschrijving van de gegevensanalyse en de reflectie ten aanzien van de validiteit, betrouwbaarheid en ethische aspecten van het uitgevoerde onderzoek. Aan het einde van dit hoofdstuk zal er sprake zijn van een voorlopig model welke in de volgende hoofdstukken geoperationaliseerd wordt.

Hoofdstuk vier beschrijft de uitvoering en de resultaten van het empirische onderzoek. Hierin zal expliciet gekeken worden naar de invulling van de risico's in het ontwikkelde raamwerk, de validatie en hoe het zal worden geoperationaliseerd.

Hoofdstuk vijf beschrijft uiteindelijk de discussie en vervolgens worden de conclusies getrokken uit het onderzoek. Hier wordt ook het definitieve model getoond. Afsluitend zijn er aanbevelingen voor de praktijk en voor eventueel verder onderzoek.

2. Theoretisch kader

Dit onderzoek is geïnspireerd op de richtlijnen uit Design Science Research (DSR) (Hevner et al., 2004), waarbij er voor het literatuuronderzoek (rigor) gebruik is gemaakt van de aspecten zoals benoemd door Saunders (Saunders, Lewis, & Thornhill, 2016). De praktijkrelevantie (relevance) is in de probleemstelling hierboven beschreven. Het in dit hoofdstuk ontwikkelde theoretisch kader is het artefact van dit onderzoek. Het doel hiervan is inzicht te verschaffen in de reeds bestaande wetenschappelijke visies die ontwikkeld zijn op cybersecuritygebied en dan met name vanuit de lens van de MKB-ondernemer. Dit artefact wordt vervolgens geoperationaliseerd en gevalideerd in latere hoofdstukken.

De gevonden literatuur uit het vakgebied alsook de theorie die uit andere vakgebieden gebruikt kan worden, moet leiden tot antwoorden op de gedefinieerde hoofd- en deelvragen.

2.1. Onderzoeksaanpak

Het theoretische deel (rigor) van DSR wordt in de basis uitgevoerd door een literatuuronderzoek. Het literatuuronderzoek volgt grotendeels het iteratieve proces zoals beschreven door Saunders. (Saunders et al., 2016). De uitkomsten uit het literatuuronderzoek zullen vervolgens leiden tot het opstellen van een model. Dit model zal gedurende het empirische deel van het onderzoek geoperationaliseerd worden.

Het theoretisch kader richt zich specifiek op het beantwoorden van de eerste helft van de deelvragen die geformuleerd zijn in de eerder beschreven opdrachtformulering. Specifiek voor het literatuuronderzoek gaat het dan om het beantwoorden van de volgende deelvragen:

1.1. *Welke modellen zijn er al bekend ter beoordeling van de 'mate van volwassenheid procesinrichting' en welk model kan als determinant dienen voor het MKB?*
1.2. *Welke modellen zijn er al bekend ter beoordeling van de 'mate van digitalisering' en welk model kan als determinant dienen voor het MKB?*
1.3. *Welke modellen zijn er al bekend ter beoordeling van de genomen cybersecuritymaatregelen en welk model kan als determinant dienen voor het MKB?*

Hierbij wordt er dus nadrukkelijk gezocht naar de indicatoren voor de verschillende volwassenheidsaspecten en niveaus ten opzichte van de categorieën zoals benoemd in de deelvragen. De verbinding met de risico's voor de bedrijfsvoering zal in het daadwerkelijke onderzoek gedestilleerd worden uit de interviews en deze zullen in het laatste hoofdstuk gekoppeld worden aan het ontwikkelde raamwerk. Na het koppelen aan het raamwerk zullen de gedefinieerde risico's gevalideerd worden door het ontwikkelde raamwerk voor te leggen aan de respondenten middels een korte enquête.

Bij het literatuuronderzoek is gebruik gemaakt van zowel Engelse als Nederlandse vertalingen van deze zoektermen. Het overgrote deel van de gevonden literatuur uit de zoekslagen met Nederlandse termen was informatief en niet wetenschappelijk en is daarom vooral gebruikt in de onderbouwing van de praktijk.

Geraadpleegde bronnen voor het literatuuronderzoek:
- Google Scholar
- Universiteitsbibliotheek OU (met alle hieraan gekoppelde databases)
- In sommige gevallen "sneeuwbalmethode"; doorzoeken in de referenties van gevonden artikelen.

Per deelvraag zijn er specifieke query's opgesteld om tot relevante wetenschappelijke artikelen te komen. In onderstaand overzicht zijn alleen de Engelstalige zoektermen benoemd omdat deze de meest relevante artikelen hebben opgeleverd. De ontwikkeling van deze zoektermen is tot stand gekomen middels de methode van Dreher en Dreher (Dreher & Dreher, 2011).

Deelvraag: 1.1. Welke modellen zijn er al bekend ter beoordeling van de 'mate van volwassenheid procesinrichting' en welk model kan als determinant dienen voor het MKB?
Query: 'maturity AND business processes' / 'Level business processes' / 'SME business processes'

Deelvraag: 1.2. Welke modellen zijn er al bekend ter beoordeling van de 'mate van digitalisering' en welk model kan als determinant dienen voor het MKB?
Query: 'measure business ICT' / 'IT maturity level' / 'Digital maturity SME' / 'Business IT Alignment'

Deelvraag: 1.3. Welke modellen zijn er al bekend ter beoordeling van de genomen cybersecuritymaatregelen en welk model kan als determinant dienen voor het MKB?
Query: 'cyber security SME' / 'cyber security maturity' / 'cyber security level' / 'cyber security metrics' / 'cyber security index'

2.2. Uitvoering

Voor de uitvoering van de literatuurstudie is er gebruik gemaakt van het erkende PRISMA protocol (Moher, Liberati, Tetzlaff, & Altman, 2009) en bij het opslaan van de gevonden artikelen is er gebruikt gemaakt van de software van 'Endnote'. Per deelvraag is het flowdiagram van het PRISMA-protocol ingevuld om zo aan te geven welke relevante artikelen er gevonden zijn.

Deelvraag: 1.1. Mate van volwassenheid procesinrichting **PRISMA Flow Stappen**	**Aantal artikelen**
Records identified through database searching (n=)	35
Additional records identified through other sources (n=)	44
Records after duplicates removed (n=)	64
Records screened (n=)	26
Full-text articles assessed for eligibility (n=)	20
Studies included in qualitative synthesis (n=)	6

Deelvraag: 1.2. Mate van digitalisering **PRISMA Flow Stappen**	**Aantal artikelen**
Records identified through database searching (n=)	96
Additional records identified through other sources (n=)	97
Records after duplicates removed (n=)	134
Records screened (n=)	35
Full-text articles assessed for eligibility (n=)	22
Studies included in qualitative synthesis (n=)	8

Deelvraag: 1.3. Beoordeling van genomen cybersecuritymaatregelen **PRISMA Flow Stappen**	**Aantal artikelen**
Records identified through database searching (n=)	24
Additional records identified through other sources (n=)	94
Records after duplicates removed (n=)	58
Records screened (n=)	28
Full-text articles assessed for eligibility (n=)	17
Studies included in qualitative synthesis (n=)	8

2.3. Resultaten en conclusies

In deze paragraaf worden de uitkomsten van het literatuuronderzoek beschreven. Per deelvraag is er een aparte paragraaf gewijd aan de conclusies die getrokken kunnen worden uit de gevonden literatuur. In paragraaf 2.3.1. wordt een uiteenzetting van de gevonden modellen ter beoordeling van de mate van volwassenheid van de procesinrichting gegeven. Aan de hand van deze gevonden modellen wordt er een volwassenheidsthermometer voor het MKB beschreven. Paragraaf 2.3.2. geeft weer welke modellen er gevonden zijn ter beoordeling van de mate van digitalisering van een organisatie en de toepasbaarheid daarvan op het MKB. Uit deze modellen wordt dan een digitalisatiethermometer voor het MKB geëxtraheerd. De beoordeling van de modellen die de genomen cybersecuritymaatregelen van een organisatie toetst wordt in paragraaf 2.3.3. gebruikt om de derde thermometer te ontwikkelen. Paragraaf 2.3.4. zal vervolgens de opsomming van de ontwikkelde thermometers en antwoorden op de eerste drie deelvragen weergeven. Waarna in paragraaf 2.3.5. dit alles in een visueel model wordt gepresenteerd.

2.3.1. Mate van volwassenheid procesinrichting

Volwassenheid van bedrijfsprocessen is een concept dat al tientallen jaren gebruikt wordt om de effectiviteit en mate van proces integratie van een organisatie aan te tonen (Hammer, 2007). Om een antwoord te kunnen geven op deelvraag 1.1. is het van te belang te onderkennen welke modellen van toepassing kunnen zijn. Niet elk bestaand model heeft de karakteristieken om bedrijfsproces-volwassenheid te bepalen aan de hand van eventuele cyber risico aspecten. Daarnaast zijn er de afgelopen decennia tientallen Business Process Management Maturity (BPMM) modellen ontwikkeld zonder dat deze op een goede wijze zijn gevalideerd (Tarhan et al., 2016). Om te bepalen welke BPMM's voor dit onderzoek een goede leidraad kunnen bieden voor het bepalen van de mate van volwassenheid, is het wenselijk om te kijken naar het primaire doel waarvoor een BPMM is opgesteld. Hierin is onderscheid te maken in BPMM's die bestemd zijn om enkele of een aantal processen binnen een organisatie te beoordelen en BPMM's die bestemd zijn om alle processen binnen een onderneming te beoordelen (Jeston, 2014). In dit onderzoek wordt gekeken naar modellen die de organisatie als geheel beoordelen waardoor enkel de BPMM's overblijven die hierop focussen. Om ervoor te zorgen dat alleen gevalideerde modellen worden gebruikt zal gebruik gemaakt worden van de BPMM Smart-Selector (Van Looy, De Backer, Poels, & Snoeck, 2013). Door bovenstaande methode is tot een selectie van onderstaande modellen gekomen die gebruikt kunnen worden voor dit onderzoek. Deze modellen zijn ook aangehaald in eerder uitgevoerd onderzoek (Röglinger, Pöppelbuß, & Becker, 2012).

	Scope*	Lowest Maturity Level	Upmost Maturity Level
Process Management Maturity Assessment (PMMA) (Rohloff, 2009a, b)	BPM & P	*Initial:* Processes are not defined; success depends on certain specialists; schedule, quality and costs are not predictable.	*Optimizing:* Processes are analyzed, optimized and adjusted to changes in market requirements systematically. Benchmarking and mistake avoidance is pursued.
BPO Maturity Model (BPOMM) (McCormack, 2007, McCormack et al., 2009)	BPM & P	*Ad-hoc:* Processes are unstructured and ill-defined. No process measures exist. Organizational structures are based on traditional functions.	*Integrated:* The organization cooperates with vendors and suppliers on process level. Organizational structures are based on processes. There are deeply imbedded process measures.
Process and Enterprise Maturity Model (PEMM) (Hammer, 2007)	BPM & P	*P-1/E-1 (examples):* The process has not been designed on an end-to-end basis. Fragmented legacy IT systems support the process.	*P-4/E-4 (examples):* Process design fits with customer and supplier processes. Modular IT architecture exists.
Process Maturity Ladder (PML) (Harmon, 2004, 2007)	BPM & P	*Initial:* Processes are not defined.	*Optimizing:* Processes are measured and managed. Process improvement teams exist.
Business Process Maturity Model (BPMM-OMG) (Weber et al., 2008)	BPM & P	*Initial:* There is "fire-fighting management". Success depends on the competence and heroics of individuals and not on the use of proven processes.	*Innovating:* There is "change management". Approaches to defect and problem prevention as well as continuous and innovative improvements are in place.
Business Process Maturity Model (BPMM-Lee) (Lee et al., 2007)	BPM & P	*Initial:* Processes are managed in an ad-hoc manner.	*Optimizing:* Processes are proactively monitored and controlled. Process performance data is systematically used for improvements.

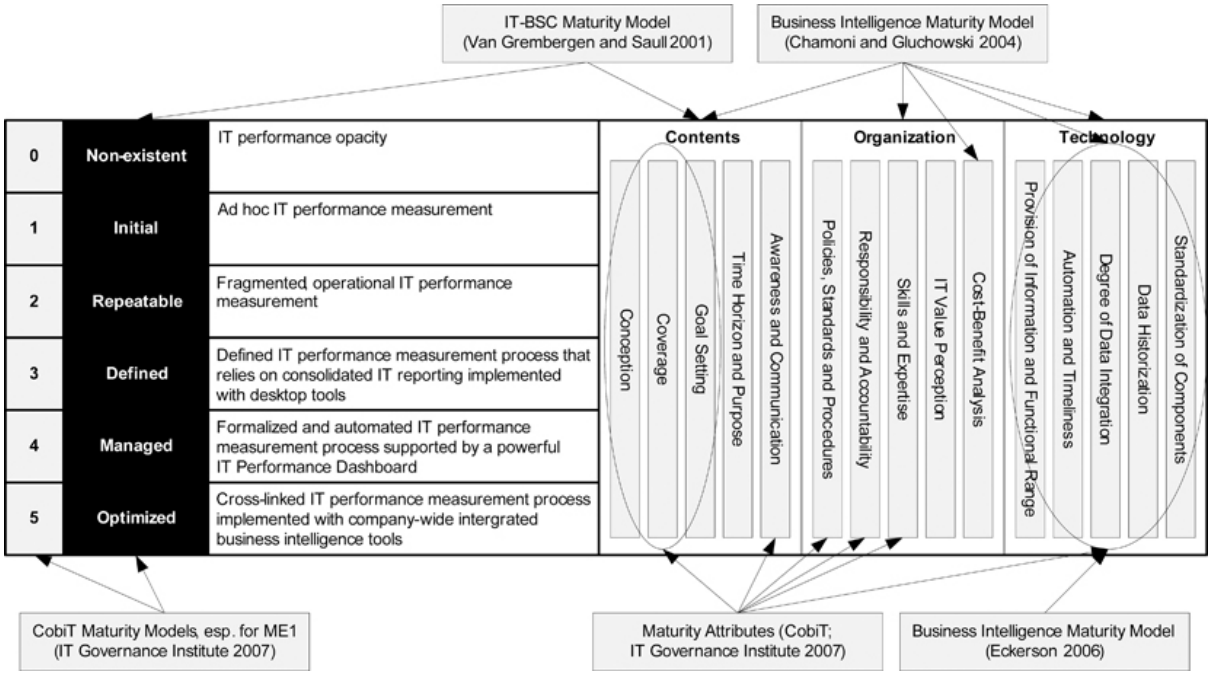
* BPM = Business Process Management, P = Processes in general

Overzicht van Proces Volwassenheid modellen (Röglinger et al., 2012)

Vanwege de kleine verschillen in vier van de zes modellen, is er in dit onderzoek gekozen om in ieder geval de schaalverdeling van deze vier (PMMA, PML, BPMM-OMG en BPMM-Lee) modellen te volgen voor de bouw van het model. Specifiek voor dit onderzoek wordt er verder gebruik gemaakt van het PMMA-model (Rohloff, 2011) vanwege de focus op een aantal categorieën die specifiek met IT te maken hebben en de vertaalbaarheid naar kleinere organisaties.

2.3.2. Mate van digitalisering

Om duidelijk te krijgen hoeveel risico een onderneming loopt op het gebied van cyberdreigingen is het belangrijk om te bepalen hoe divers de aanvalsvectoren (manieren die een aanvaller kan gebruiken om een systeem binnen te komen) van de organisatie zijn. Daarvoor zal er gekeken worden hoe groot de IT ondersteuning en toepassingen zijn van een organisatie (Kotarba, 2017; Müller, von Thienen, & Schröder, 2004). Na alle bedrijfsvolwassenheidsmodellen is er ook steeds meer aandacht voor de mate van digitalisatie die een onderneming bereid is door te voeren (Hamidi, Aziz, Shuhidan, Aziz, & Mokhsin, 2018). Deze mate van digitalisatie brengt zowel kansen als bedreigingen met zich mee (Chen, Jaw, & Wu, 2016; Henderson & Venkatraman, 1999). Om hier inzicht in te krijgen is het van belang om een goed model te gebruiken voor de ontwikkeling van het raamwerk. In het overzichtsonderzoek naar de ontwikkeling van 'Maturity models for IT management' (Becker, Knackstedt, & Pöppelbuß, 2009) is er gekeken naar de reeds bestaande volwassenheidsmodellen voor digitalisatie en Business Intelligence. In onderstaande tabel is het ITPM-model van Becker et al. (2009) gevisualiseerd en deze wordt in dit onderzoek gebruikt om de niveaus te bepalen.



Overzicht van karakteristieken van IT volwassenheidsmodellen(Becker et al., 2009)

Vervolgens is er gekeken naar de diverse karakteristieken (Hribar Rajterič, 2010; Müller et al., 2004) van de verschillende modellen die gebruikt zijn om tot het ITPM-model te komen om antwoord te kunnen geven op deelvraag 1.2. Het ITPM-model laat duidelijk zien dat de attributen die ontleend zijn uit het CobiT-model, normaliter bedoeld voor het bepalen van de volwassenheid van IT-governance, het meest gespecificeerd en verdeeld over de drie hoofdcategorieën zijn. De keuze voor het ITPM-model is voornamelijk vanwege deze attributen die het model gebruikt voor het bepalen van het digitalisatieniveau en de gelijkenis van de niveaubepalingen bij PMMA zoals gekozen is bij de procesvolwassenheid graadmeter. De attributen die CobiT gebruikt en in het ITPM-model zijn overgenomen zijn in tegenstelling tot veel andere modellen beter verdeeld over de verschillende PPT (Personen Processen en Technologie) aspecten van een onderneming en daarnaast zijn ze wel tastbaar en inzichtelijk te maken om bruikbaar te zijn voor een MKB.

2.3.3. Beoordeling van genomen cybersecuritymaatregelen

Om te bepalen hoe goed de cybersecurity van een onderneming is moet er gekeken worden naar de operationele processen, security capaciteiten en de te beschermen systemen (Donaldson, Siegel, Williams, & Aslam, 2015). Voor het te ontwikkelen model wordt er gestart met de bevindingen uit het overkoepelende onderzoek (PVO & Brightlands, 2018). Tijdens de zoektocht naar het antwoord op deelvraag 1.3.: '*Welke modellen zijn er al bekend ter beoordeling van de genomen cybersecuritymaatregelen en welk model kan als determinant dienen voor het MKB?*' wordt op basis van het overkoepelende onderzoek het volwassenheidsniveau van de MKB-onderneming bepaalt, wat bijdraagt aan een verdere ontwikkeling van de daaruit ontwikkelde weerbaarheidsscan. Er blijken drie beschikbare onderzoeken naar voren te komen die, bij de bepaling van het cybersecurity volwassenheidsniveau, de verschillende veelgebruikte modellen vergelijken (de Bruin & von Solms; Le & Hoang, 2016; Rea-Guaman, Sánchez-García, San Feliu, & Calvo-Manzano, 2017). Uit het onderzoek van Le & Hoang is de tabel die hieronder getoond wordt verkregen. De modellen die door NIST (Almuhammadi & Alsaleh, 2017) en CERT (Butkovic & Caralli, 2018) zijn ontwikkeld zijn voor dit onderzoek minder toepasbaar vanwege de diepgang en complexiteit waarin zij categorieën en niveaus van cyber security beschrijven. Dit is voor het MKB te uitgebreid om te gebruiken.

Het model dat wel toepasbaar lijkt voor de ontwikkeling van ons model is het Information Security Framework (ISF) van IBM (Buecker, Borrett, Lorenz, & Powers, 2010) vanwege de duidelijke stappen en de schaalbaarheid van het model.

	Cyber Security Maturity Models (CSM2)	Organizations or Author	Purposes and Strengths	Maturity Levels				
				1	2	3	4	5
1	Information Security Evaluation Maturity Model (ISEM), 2000	City Group	Security awareness and evaluation	Complacency	Acknowledgement	Integration	Common practice	Continuous improvement
2	Systems Security Engineering Capability Maturity Model (SSE-CMM), 2001	The US National Security Agency (NSA)	Evaluation of software security engineering processes	Performed informally	Plan and track	Well defined	Control	Continuous improvements
3	Information security management system (ISMS-ISO 27001), 2005	ISO	Information security risk management through security standards	Performed	Managed	Established	Predictable	Optimized
4	Information Security Management Maturity Model (ISM3), 2007	ISM3 Consortium	Prevent and mitigate incidents and Optimise the use of information, money, people, time and infrastructure	Undefined	Defined	Managed	Controlled	Optimized
5	Information Security Maturity Model (ISM2), 2007	NIST-PRISMA	Provides a framework for review and measure the information security posture of an information security program	Polices	Procedures	Implemented	Tested	Integrated
6	Gartner's Information Security Awareness Maturity Model (GISMM), 2009	Gartner	Security awareness, and risk management in large international organizations	Blissful ignorance	Awareness	Corrective	Operations excellence	
7	Information Security Framework (ISF), 2009	IBM	Security gap analysis between business and technology	Initial	Basic	Capable	Efficiency	Optimizing
8	Resilience Management Model (RMM), 2010	CERT	A capability-focused process model for managing operational resilience	Incomplete	Performed	Managed	Defined	
9	Community Cyber Security Maturity Model (CCSMM), 2011	White	Community effort and communication capability in communities	Initial	Advanced	Self-Assessed	Integrated	Vanguard
10	NICE's Cyber Security Capability Maturity Model, 2012	The US DHS	Workforce planning for cyber security best practices	Limited	Progressing	Optimized		
11	Cyber Security Framework (CSF-NIST), 2014	NIST	Improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators	Identify	Protect	Detect	Respond	Recover
12	Cyber Security Capability Maturity Model (C2M2), 2015	Curtis	Assessment of implementation and management in Critical Infrastructure	Not performed	Initiated	Performed	Managed	

Analyse van Cyber Security Maturity modellen (Le & Hoang, 2016)

2.3.4. Conclusies naar aanleiding van de literatuur

Volgens het principe van Capability Maturity Model (CMM) zijn volwassenheidsmodellen opgebouwd uit 5 levels (Humphrey, 1988). Naar analogie van CMM volgen we 5 levels voor zowel de procesvolwassenheid als ook de mate van digitalisatie: Ad-Hoc, Engaged, Structured, Managed, Optimized. De invulling van deze levels wordt gedaan aan de hand van het PMMA-model voor de procesvolwassenheid en door het ITPM-model voor de mate van digitalisatie.

Voor elk van de modellen is een matrix gebouwd met daarbij op de horizontale as de volwassenheidsniveaus en op de verticale as de categorieën waarop de gekozen modellen het niveau bepalen. Vervolgens zijn er in de corresponderende matrix omschrijvingen van de te meten aspecten van deze categorieën beschreven. Door het invullen van elk van deze matrixen kan een MKB zelf onderkennen op welk niveau zij zich bevinden ten opzichte van procesvolwassenheid en mate van digitalisatie.

De specifieke koppeling van de vragen aan de maturity levels en daarmee dus de eerste stap in de operationalisering van het model is uitgewerkt in 'Bijlage B. Operationalisering Dimensies Raamwerk'. Een visualisatie is hieronder weergegeven.

Proces Volwassenheid		De volwassenheid van een organisatie kan bepaald worden door het gebruik van onderstaande tabel. Indien een bewering Grotendeels waar is (minstens 75% waar) wordt het vlak gevuld met de kleur groen; als de bewering Deels waar/Deels niet waar is (tussen 25% en 75% waar) wordt het vlak gevuld met de kleur geel; en als de bewering Grotendeels niet waar is (minder dan 25% waar) dan wordt het vlak gevuld met de kleur rood. Aan de hand van het totaaloverzicht kan het generieke volwassenheidsniveau van de organisatie bepaald worden.						GROEN: Grotendeels waar	GEEL: Deels waar/Deels niet waar	Rood: Grotendeels niet waar		
		Ad-Hoc	Engaged	Structured	Managed	Optimized		Ad-Hoc	Engaged	Structured	Managed	Optimized
Ontwerp	Doel	Het doel van sommige processen is bekend.	Het doel van alle processen is bekend binnen het bedrijf.	Alle processen zijn van begin tot einde ontworpen om maximale effectiviteit te garanderen.	De processen zijn zo ontworpen dat zij matchen met elkaar en de aanwezige IT-systemen.	De processen in het bedrijf zijn volledig in lijn met klant en leveranciers processen en bevorderen maximale effectiviteit en efficiency.						
	Documentatie	Er is geen documentatie aanwezig van de processen.	De meeste van de processen zijn helder en zijn gedocumenteerd.	Alle processen zijn beschreven en er is duidelijkheid hoe deze van begin tot einde verlopen.	De documentatie beschrijft de correlatie tussen de verschillende bedrijfsprocessen en de afhankelijkheden zijn duidelijk.	Er is een digitale database met alle bedrijfsprocessen, de koppelingen en er zijn meetbare prestatie indicatoren.						
Gebruikers	Kennis	Sommige spelers in het proces kennen de structuur.	Alle spelers in een proces zijn op de hoogte van de procesflow.	Kennis van de bedrijfsprocessen is wijdverspreid binnen het bedrijf.	Medewerkers zijn bekend met en opgeleid in proces verbeterende technieken.	Medewerkers gaan actief op zoek naar verbetermogelijkheden van processen en er is de ruimte om deze aan te passen.						
Eigenaar	Identiteit	Proces eigenaren zijn niet of nauwelijks gedefinieerd.	Proceseigenaren zijn bekend.	De rol van Proceseigenaar is officieel gecreëerd en deze zijn verantwoordelijk voor verbeteringen.	De proceseigenaar heeft het proces als hoofddoel en heeft de bevoegdheid en middelen om verbeteringen door te voeren.	De proceseigenaar heeft een visie en roadmap voor het bestaande proces en hij/zij is onderdeel van het besluitvormingsproces van het bedrijf.						
ICT infrastructuur	IT-Systemen	Processen worden nauwelijks ondersteund door IT-systemen.	Processen worden ondersteund door specifiek IT-componenten.	Een geïntegreerd IT-systeem ondersteund de processen, welke ook ontworpen is met oog op het proces.	Processen worden volledig ondersteund door IT oplossingen en deze IT-systemen zijn in beperkte mate met elkaar verbonden.	Er is een volledig geïntegreerd systeem, moduleerbaar en volgens standaarden ontwikkelde IT-architectuur.						
Statistieken	Definitie	Er zijn geen statistische indicatoren.	Er is in beperkte mate inzicht op de werken van de processen.	De processen hebben indicatoren die de verschillende vereisten meten.	De processen worden door het hele proces heen gemonitord op de werking.	De processtatistieken worden cross-proces volledig bijgehouden en hier wordt ook op gestuurd.						

Procesvolwassenheidsmatrix op basis van het PMMA-model.

Mate van Digitalisatie		De volwassenheid van een organisatie kan bepaald worden door het gebruik van onderstaande tabel. Indien een bewering Grotendeels waar is (minstens 75% waar) wordt het vlak gevuld met de kleur groen; als de bewering Deels waar/Deels niet waar is (tussen 25% en 75% waar) wordt het vlak gevuld met de kleur geel; en als de bewering Grotendeels niet waar is (minder dan 25% waar) dan wordt het vlak gevuld met de kleur rood. Aan de hand van het totaaloverzicht kan het generieke volwassenheidsniveau van de organisatie bepaald worden.					GROEN: Grotendeels waar	GEEL: Deels waar/Deels niet waar	Rood: Grotendeels niet waar		
		Ad-Hoc	Engaged	Structured	Managed	Optimized	Ad-Hoc	Engaged	Structured	Managed	Optimized
Middelen	Apparatuur/Hardware	Middelen worden zonder groter plan of visie aangeschaft.	Er is in beperkte mate beleid voor de aanschaf van middelen.	Middelen worden volgens een bepaalde visie en standaard aangeschaft en ingezet met het oog op de specifieke bedrijfsbehoeften.	Alle hardware wordt aangeschaft en ingezet volgens een vooraf opgesteld plan en aan de hand van de geformuleerde architectuur.	Er wordt geen hardware toegestaan die niet voldoet aan de visie en standaarden van het bedrijf.					
	Software	Software wordt ad-hoc gekocht dan wel gedownload.	Software wordt waar mogelijk bedrijfsbreed beoordeelt en vervolgens aangeschaft.	De software ondersteund zo effectief mogelijk de verschillende processen binnen het bedrijf.	De software van de verschillende processen is deels met elkaar verbonden en hier is in sommige mate een vorm van analyse op uit te voeren.	Er is sprake van ERP-systeem achtige software welke door alle processen heen in verbinding staat met elkaar. Hier wordt actief op gemonitord en verbeteringen voor de processen worden door de software mogelijk gemaakt.					
	Automatisering	Er is praktisch geen sprake van automatisering.	Bepaalde processen zijn verrijkt met IT componenten	Bepaalde processen zijn gedigitaliseerd.	Sommige processen zijn geautomatiseerd.	Alle processen zijn volledig geautomatiseerd en deze processen zijn met elkaar verbonden.					
Kennis	Kennis	Er is praktisch geen kennis over de aanwezige IT systemen binnen het bedrijf.	Er is beperkte kennis van de IT systemen aanwezig in het bedrijf.	Er is kennis van de aanwezige systemen en er wordt in beperkte mate ook gedaan aan kennisopbouw.	Er is een actief programma binnen de organisatie om kennis op te bouwen over IT en er zijn voldoende scholingsmogelijkheden voor het personeel.	Het kennis niveau binnen de organisatie zit op een zeer hoog niveau en er wordt onderzoek gedaan naar toekomst mogelijkheden.					
Architectuur	Proces	Er is geen of alleen ad-hoc architectuurproces.	De IT architectuur is beschreven, hier zijn ook duidelijke rollen in aangegeven.	De IT-architectuur is goed uitgewerkt en zowel IT-personeel als het management is hiervan op de hoogte.	De IT-architectuur maakt onderdeel uit van de bedrijfscultuur en wordt actief gemonitord op zijn prestaties.	Er wordt continue gezocht naar optimalisatie van de IT-architectuur en verbeteringen van het proces worden doorgevoerd.					
Management	Documentatie	De gebruikte ICT binnen het bedrijf is niet gedocumenteerd.	Er is een soort van overzicht van de aanwezige hardware en software.	Er is een goed gedocumenteerd overzicht van de aanwezige hardware en software, en dit wordt ook actief bijgehouden en gecontroleerd.	Hardware en software worden actief gemanaged door een beheerorganisatie.	Er is volledig overzicht van de bedrijfsbrede middelen, hier wordt actief beheer op gepleegd.					
	Doelstelling	Er zijn geen doelstelling geformuleerd voor de gebruikte technologie.	Er is in beperkte mate inzicht in de doelstellingen die IT moet ondersteunen.	In grote mate zijn doelstellingen geformuleerd welke door IT behaald moeten worden. Hierbij is er een koppeling gemaakt naar de bedrijfsprocessen die essentieel zijn voor de organisatie.	Er is een duidelijk organisatie doel voor ogen welke ondersteund moet worden door de aanwezige IT middelen. Deze middelen worden proces overstijgend ingezet.	De aanwezige IT middelen en bedrijfsprocessen vormen een intrinsiek geheel en worden in nauwe coördinatie met elkaar constant verbeterd.					

Mate van digitalisatie op basis van het ITPM-model

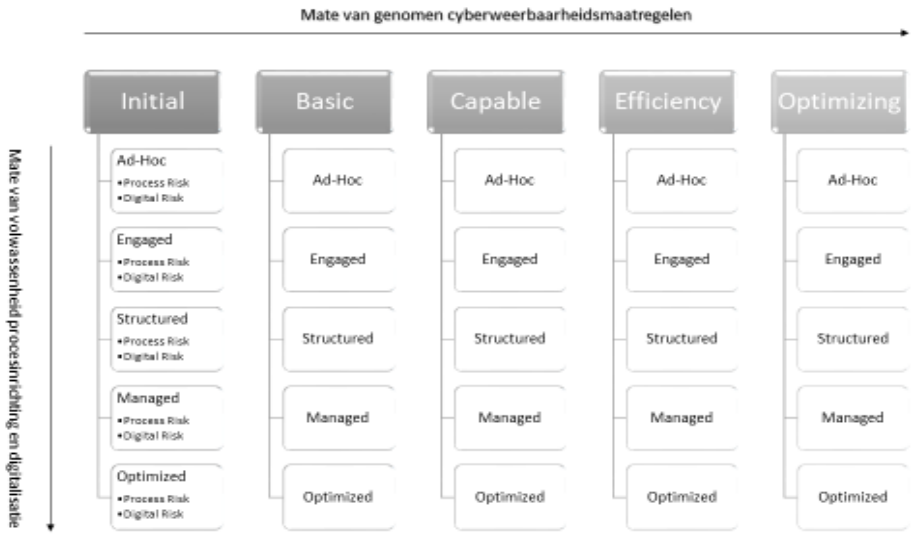
Om de cybervolwassenheid van een MKB te bepalen maken we gebruik van elementen uit het onderzoek van de PVO Limburg. Om hier vervolgens een classificatie op toe te passen en de componenten te kiezen per niveau wordt gebruik gemaakt van de schaalverdeling van het Information Security Framework (ISF), te weten: Initial, Basic, Capable, Efficiency en Optimizing. Ook hier is er gebruik gemaakt van te kwantificeren aspecten zodat een MKB zelf kan inschatten in welke mate zij cybersecurity hebben toegepast binnen het bedrijf.

Mate van Cybersecurity		De volwassenheid van een organisatie kan bepaald worden door het gebruik van onderstaande tabel. Indien een bewering Grotendeels waar is (minstens 75% waar) wordt het vlak gevuld met de kleur groen; als de bewering Deels waar/Deels niet waar is (tussen 25% en 75% waar) wordt het vlak gevuld met de kleur geel; en als de bewering Grotendeels niet waar is (minder dan 25% waar) dan wordt het vlak gevuld met de kleur rood. Aan de hand van het totaaloverzicht kan het generieke volwassenheidsniveau van de organisatie bepaald worden.						GROEN: Grotendeels waar	GEEL: Deels waar/Deels niet waar	Rood: Grotendeels niet waar		
		Initial	Basic	Capable	Efficiency	Optimizing		Initial	Basic	Capable	Efficiency	Optimizing
Identificeren	Inzicht in middelen	Er is geen overzicht en/of inzicht in de aanwezige hardware en software.	Er is een soort van overzicht van de aanwezige hardware en software.	Er is een goed gedocumenteerd overzicht van de aanwezige hardware en software, en dit wordt ook actief bijgehouden en gecontroleerd.	Hardware en software worden actief gemanaged door een beheerorganisatie.	Er is volledig overzicht van de bedrijfsvrede middelen, hier wordt actief beheer op gepleegd en kwetsbaarheden zijn bekend en indien mogelijk gemitigeerd.						
	Digitale voetafdruk	Er is geen overzicht van de digitale voetafdruk van het bedrijf.	Er is een globaal overzicht van de digitale voetafdruk van het bedrijf.	Er is een structureel en gedocumenteerd overzicht van alle web en social media platformen waar het bedrijf op actief is.	Er wordt actief gecontroleerd wat er zich afspeelt binnen de digitale voetafdruk van het bedrijf.	Er wordt actief op zoek gegaan naar de digitale mogelijkheden om het bedrijf te benaderen en of deze allemaal juist zijn geconfigureerd.						
Beschermen	Bescherming	Geen of sommige systemen worden voorzien van updates.	Het grootste deel van de systemen wordt regelmatig voorzien van updates. Er is een policy met betrekking tot wachtwoorden.	Het bedrijf beperkt het gebruik van verwijderbare media zoals USB-sticks en SD-kaarten. De firewall is actief. Wachtwoord policies zijn naar de huidige standaard.	Updates van besturingssystemen, applicaties en antivirussoftware wordt structureel uitgevoerd.	Toegang tot systemen en data is beschreven en alleen mogelijk voor geautoriseerde personen.						
	Awareness	Awareness van het personeel komt niet of nauwelijks aan de orde.	Awareness wordt af en toe behandelt.	Medewerkers weten cybercrime te herkennen.	Awareness komt structureel aan de orde en medewerkers weten hoe te handelen bij cybercrime.	Medewerkers worden geschoold in cybersecurity en er is een constante actieve awareness campagne.						
Opsporen	Monitoring	Antivirus is niet of nauwelijks aanwezig.	Antivirussystemen zijn grotendeels aanwezig.	Antivirussystemen zijn verplicht en up to date.	Het bedrijf scant actief op malware en andere dreigingen.	Het bedrijf maakt gebruik van IDS/IPS en monitored zijn systemen continue.						
Reactie	Mitigatie	Er is geen of nauwelijks besef wat er gedaan moet worden bij een mogelijk incident.	Er is een redelijk idee wat er gedaan moet worden bij een mogelijk incident.	Er is beschreven wat er gedaan moet worden bij een mogelijk incident en er zijn mitigerende maatregelen.	Er zijn procedures om een incident te beperken, mitigerende maatregelen zijn in place.	Na een incident wordt er analyse uitgevoerd op de herkomst en oorzaak van het incident. Er wordt lering uit getrokken en actief op zoek gegaan naar nieuwe kwetsbaarheden en de impact daarvan op het bedrijf.						
Herstellen	Herstel	Er worden geen back-ups gemaakt, of alleen sporadisch.	Het bedrijf heeft beleid bepaald ten aanzien van het maken van back-ups.	Het bedrijf maakt regelmatig een back-up van lokale data.	Het bedrijf maakt regelmatig een back-up van alle relevante data in de Cloud en off-site.	De back-up kan worden teruggezet. Het terugzetten van een back-up is getest.						

Mate van genomen cybersecuritymaatregelen op basis van het ISF

2.3.5. Voorlopig model & operationalisering

Het voorlopige model maakt gebruik van de volwassenheidsniveaus die uit de literatuur zijn gekozen vanwege de toepasbaarheid voor het MKB. Deze zijn in de vorige paragraaf gepresenteerd met de daarbij behorende invulmatrixen welke de karaktereigenschappen weergeven. Onderzoek heeft in het verleden al deels gekeken naar het verband tussen proces en risico's voor het MKB (Lim, 2010) en tussen IT en risico's (Trim & Lee, 2016), maar nog niet naar een combinatie van de drie gedefinieerde constructen. De horizontale as van het voorlopige model geeft het niveau van de genomen cyberweerbaarheidsmaatregelen weer. Op de verticale as is de schaalverdeling van de procesvolwassenheid en van de mate van digitalisatie samen weergegeven, deze combinatie is gekozen vanwege het sterk overeenkomende karakter van de niveau beschrijvingen. Nu we dit weten komen we aan de hand van de constructen tot het netto risico oftewel de restrisico's. Dit zijn rest risico's omdat dit de risico's voor de bedrijfsvoering zijn na het in beschouwing nemen van de genomen cyberweerbaarheidsmaatregelen, ook wel het nadelige effect dat dit heeft op het bedrijf. De samenkomst van het horizontale niveau en het verticale niveau zal uiteindelijk de MKB-ondernemer een beeld geven van het cyberrisiconiveau van het bedrijf. Hierdoor kan dus een antwoord gegeven worden op deelvraag 1.4. Deze specifieke restrisico's worden in het vervolgonderzoek gedestilleerd door middel van expertinterviews.



Voorlopig Model (Zie ook Bijlage A)

2.4. Doel van het vervolgonderzoek

Op basis van de gevonden literatuur is er in paragraaf 2.3.5. een voorlopig model geformuleerd om de risico's (netto risico) inzichtelijk te kunnen maken die een MKB-ondernemer loopt door onvoldoende genomen cyberweerbaarheidsmaatregelen ten opzichte van zijn procesvolwassenheid en mate van digitalisatie. De drie constructen, namelijk; procesvolwassenheid, digitalisering en genomen cybermaatregelen, die hierin beschreven zijn als thermometers moeten nog voorzien worden van de mogelijke risico's die verschillende volwassenheidsniveaus en niet genomen maatregelen met zich meebrengen. Deze risico's zullen gedestilleerd worden uit de interviews met de verschillende experts op dit onderwerp. Tijdens de interviews zal ook gebruik gemaakt worden van de Mitre Att&ck Matrix("MITRE ATT&CK MATRIX," 2020) welke in de praktijk veelvuldig gebruikt wordt om aanvalstechnieken van cybercriminelen te identificeren en te classificeren. De hierin genoemde aanvallen zullen als handvatten dienen om tijdens de interviews concrete voorbeelden te kunnen geven.

In het empirische deel van dit onderzoek is dit model voorzien van de waardering op basis van de risico's voor het MKB. Uiteindelijk zal dit model gevalideerd moeten worden om te bezien of het een bruikbaar raamwerk is voor de MKB-ondernemer om de risico's die hij loopt voor zijn bedrijfsvoering inzichtelijk te krijgen. De conclusie en de validatie van dit raamwerk zal vervolgens leiden tot de beantwoording van de centrale vraag.

3. Methodologie

Voor het uitvoeren van het empirisch onderzoek is een volgen we de opzet zoals beschreven door Verschuren & Doorewaard (Verschuren & Doorewaard, 2007). In dit hoofdstuk zal de opzet van het onderzoek beschreven worden, waarbij de nadruk zal liggen op een kwalitatief onderzoek.

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode

In het vorige hoofdstuk is er op basis van deskresearch een raamwerk ontwikkeld om antwoord te kunnen geven op de hoofdvraag van het onderzoek. Daarbij is er per construct; procesvolwassenheid, digitalisering en genomen cybermaatregelen, een schaal gecreëerd zoals getoond in paragraaf 2.3.4. De volledige schalen zijn terug te vinden in bijlage B.

Door middel van het empirische onderzoek zal invulling gegeven worden aan de factor risico's per dimensie. En daarmee zal antwoord gegeven worden op de volgende deelvragen:

2.1. *Hoe is het ontwikkelde model toe te passen op een MKB-organisatie?*
2.2. *Welke risico's zijn te verbinden aan de verschillende niveaus van het ontwikkelde model?*

Om het raamwerk van de risico's voor de bedrijfsvoering van het MKB te voorzien is het van belang dat dit met specialisten wordt geanalyseerd. Uit deze analyses worden de risico's gedestilleerd en vervolgens wordt de verbinding gemaakt met de drie dimensies van het raamwerk.

De benodigde informatie om het raamwerk te vullen kan verkregen worden door het uitvoeren van toegepast onderzoek, kwalitatief onderzoek en/of casestudy (Saunders et al., 2016). Vanwege de complexiteit is er in dit onderzoek voor gekozen om gebruik te maken van embedded case study design (Yin, 2003). Dit type onderzoek wordt uitgevoerd in de vorm van een kwalitatief onderzoek met het gebruik van interviews. Deze interviews worden dan gebruikt om het ontwikkelde raamwerk te operationaliseren. Daarbij worden de verschillende niveaus van risico's voorzien. De redenen (van der Voordt, 1998) waarom er wordt gekozen voor een kwalitatief onderzoek op basis van interviews zijn:

- Tijdens het interview bestaat er de mogelijkheid om met de respondent het onderwerp te verdiepen.
- Het interview is niet aan een specifieke plaats of tijd verbonden.
- In tegenstelling tot een survey of een kwantitatief onderzoek is de schrijfvaardigheid van de respondent niet van belang.
- Een kwalitatief onderzoek kan nieuwe inzichten geven die gelijk verwerkt kunnen worden in het ontwikkelde raamwerk.

Het is belangrijk dat er tijdens het onderzoek gewaakt wordt voor de eventuele valkuilen (van der Voordt, 1998) die kunnen ontstaan bij het uitvoeren van een kwalitatief onderzoek op basis van interviews, deze valkuilen zijn:

- Er kan sprake zijn van een interviewer bias (beïnvloeding van de respondent door de interviewer).
- De respondent wordt alleen door de interviewer uitgedaagd om over het onderwerp na te denken.

3.2. Technisch ontwerp: uitwerking van de methode

Tijdens het kwalitatieve onderzoek wordt er gebruik gemaakt van semigestructureerde interviews. Dit betreft een combinatie tussen diepte- en expertinterviews (Reulink & Lindeman, 2005). Deze vorm biedt de mogelijkheid om wel de structuur van de deelvragen en het model te volgen en toch ruimte te laten voor een open discussie en een verdieping op de verschillende onderwerpen. Het proces voor de uitvoering van de interviews is gedaan aan de hand van het vooraf gedefinieerde protocol (Bijlage D) wat behoort tot embedded case study Research (Brereton et al., 2008; Maimbo & Pervan, 2005; Yin, 2003). Hiervoor is gekozen om de structuur van het onderzoek te waarborgen. Vooraf is elke respondent middels een interviewopzet (Bijlage E) voorzien van de richtlijnen en voorwaarden van het interview (Baarda, de Goede, & Kalmijn, 2000). Dit om de respondent de kans te bieden zich al voor te bereiden en te voorkomen dat deze verrast wordt door de vragen.

De interviews zijn afgenomen met verschillende specialisten om de risico's in kaart te brengen. Dit betreft zowel securityspecialisten met een diepgaande technische kennis als ook securityspecialisten die meer op management en organisatieniveau werkzaam zijn. De experts zijn geselecteerd op expertise in cybersecurity/informatiebeveiliging en niet noodzakelijkerwijs op kennis van het MKB, edoch zijn er een aantal experts specifiek werkzaam in het operatiegebied van het MKB. De selectie heeft plaatsgevonden op basis van de functie, dan wel de certificeringen die een persoon doorlopen heeft. Dit alles met als insteek respondenten te selecteren die zo objectief mogelijk en tevens zo kundig mogelijk een vertaalslag kunnen maken van kwetsbaarheden naar impact. Omdat het hier een relatief homogene onderzoekspopulatie betreft was het doel om vier tot tien specialisten te interviewen en te stoppen op het moment dat er saturatie optreedt in de antwoorden. De specialisten zijn gekozen uit het professionele netwerk van de onderzoeker of op aanbeveling van respondenten na afname van een interview. De verschillende respondenten dragen bij aan het beantwoorden van de deelvragen zoals beschreven in paragraaf 1.4. en uiteindelijk dus aan het beantwoorden van de hoofdvraag en de operationalisatie van het ontwikkelde raamwerk. Tijdens het onderzoek was het mogelijk dat respondenten additionele documentatie aanleveren, deze is waar mogelijk meegenomen in de beschouwing van de geformuleerde empirische onderzoeksvragen. De interviews starten met een wat meer algemene vraagstelling over de kennis en ervaring van de respondent in relatie tot het onderzoeksonderwerp. Vervolgens is aan de hand van de verschillende raamwerkcategorieën het interview gestructureerd. Dit houdt in dat de respondent per categorie bevraagd is naar de risico's die er zijn op de verschillende volwassenheidsniveaus. Afsluitend werd de respondent nog de ruimte gegeven om risico's te benoemen die door de vraagstelling eventueel niet aan de orde zijn gekomen en heeft de respondent de ruimte gekregen te reageren op het ontwikkelde raamwerk. In de *'Bijlage F. Afgenomen interviews'* zijn de verschillende interviews uitgewerkt.

3.3. Gegevensanalyse

Tijdens de registratiefase (Wester & Peters, 2004) zijn de interviews digitaal opgenomen en zijn er aantekeningen gemaakt. Om de interviews vervolgens geschikt te maken voor analyse worden deze in de transcriptiefase uitgewerkt aan de hand van het vragenformulier '*Bijlage E. Interview opzet'* tot interviewprotocollen. Dit houdt in dat er per empirische onderzoeksvraag een samenvatting is opgesteld van de gegeven antwoorden. Vervolgens is op deze transcripten open coderen toegepast door codes aan te brengen in de transcripten. Hiervoor is gebruik gemaakt van een specifiek geschreven macro welke toegepast kon worden op de digitale transcripten. Door codering aan de hand van de deelvragen wordt gezocht naar de invulling van de risico's voor het raamwerk. Door het gebruik van codes in de transcripten is het mogelijk antwoorden beknopt te registreren. Alle

relevante antwoorden zijn voorzien van codes en verzameld in de Coderingsmatrix (Miles, Huberman, Huberman, & Huberman, 1994) (Bijlage G. Coderingsmatrix). Door middel van deze matrix was het mogelijk om gericht te gaan coderen per categorie en niveau. Vervolgens is er gekeken naar verbanden en patronen in deze codes en is selectief coderen toegepast om tot de meest benoemde risico's te komen. Door het gebruik van coderingen is het ook mogelijk geweest middels een iteratief proces na elk interview het raamwerk tegen het licht te houden en de vragen in een volgend interview nog gerichter te kunnen formuleren. De voordelen van deze aanpak zijn de diepgang en de mogelijkheid tot bijsturen tijdens het onderzoek. Hierbij moest wel gewaakt worden dat de structuur niet verloren ging en dat het onderzoek binnen het gestelde tijdspad kon worden uitgevoerd. Afsluitend zijn alle onderkende risico's nogmaals middels een enquête aan alle respondenten verstuurd om te toetsen om deze in lijn zijn met de antwoorden die de respondenten tijdens de interviews gegeven hebben.

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

3.4.1. Validiteit

Bij de validiteit van een onderzoek is het belangrijk dat de onderzoeksmethode en resultaten correct zijn (Saunders et al., 2016). Dat betekent dat de methode die gebruikt wordt ook de bedoelde antwoorden moet kunnen generen en dat de resultaten ook antwoord geven op de gestelde hoofd- en deelvragen. Door het geoperationaliseerde raamwerk als leidraad voor de interviews te gebruiken wordt de onderzoeker in staat gesteld het interview te structuren aan de hand van de geformuleerde onderzoeksvragen. Daarnaast worden de risico's die genoemd zijn door de specialisten ook geverifieerd door deze, na eenmaal toegevoegd te zijn aan het model, nogmaals voor te leggen aan alle specialisten voor review. Daarmee wordt tevens antwoord gegeven op de laatste deelvraag: *Op welke manier is de validiteit van het model te meten?*

Een aantal aspecten die de validiteit zouden kunnen benadelen en hoe deze in het onderzoek worden geminimaliseerd zijn;

•Non-response: Het niet beschikbaar zijn van respondenten. Dit kan natuurlijk altijd gebeuren en daarom is ervoor gekozen om voor dit onderzoek in elke categorie van respondenten een aantal alternatieven te hebben.

•Self-selection: De kans bestaat dat het selecteren van de respondenten door de onderzoeker alleen, geen goede afspiegeling is van de benodigde expertises. Dit zal tijdens de interviews ook met de respondenten worden besproken, waarna eventueel nog aanpassingen gedaan kunnen worden in de af te nemen interviews.

3.4.2. Betrouwbaarheid

De betrouwbaarheid van het onderzoek is de mate waarin het onderzoek dezelfde resultaten genereert als het door een andere onderzoeker op dezelfde methode wordt uitgevoerd. In het geval van een kwalitatief semigestructureerd onderzoek zoals hier uitgevoerd is blijft dit een lastig punt. Er bestaat altijd het gevaar van interviewer bias en de invloed van een keuze van geïnterviewden. Het kan voorkomen dat de respondent zich laat beïnvloeden door de vragen of dat de onderzoeker subjectief is in het formuleren van de antwoorden. Dit wordt geminimaliseerd door de interviews op te nemen en achteraf de transcripties aan de respondent ter goedkeuring voor te leggen.

Tevens wordt de betrouwbaarheid ook vergroot door de mate van afhankelijkheid van toeval te verkleinen. Dit risico wordt geminimaliseerd door een zo breed mogelijke groep van respondenten te interviewen. Zodat bijvoorbeeld niet alleen risico's maar ook bruikbaarheid en dergelijke worden meegenomen in de beoordeling.

3.4.3. Ethische aspecten

Om ervoor te zorgen dat het onderzoek wordt uitgevoerd volgens de ethische principes van onderzoek (Saunders et al., 2016) is het van belang dat er gelet wordt op de integriteit en objectiviteit van de onderzoeker en de anonimiteit van de respondenten. Het mag niet zo zijn dat antwoorden gestuurd worden door de onderzoeker. Daarnaast is het van belang dat geen van de respondenten schade kan oplopen door het uitgevoerde onderzoek. Dit wordt gegarandeerd door het anonimiseren van de transcripten als ook goedkeuring van de transcripten door de respondenten voordat deze worden opgenomen in de bijlagen.

4. Resultaten

4.1. Introductie

Het empirische deel van dit onderzoek heeft als doel het ontwikkelde model te voorzien van restrisico's (de operationalisatie van het raamwerk) voor het MKB op basis van de genomen cybersecuritymaatregelen en tevens de volledigheid en juistheid van het model te toetsen. Het proces dat is gekozen om hiertoe te komen is het Case Study Protocol (Maimbo & Pervan, 2005; Yin, 2003). Om dit te kunnen volgen is gebruik gemaakt van een template die ontwikkeld is voor het gebruik bij een Case Study (Brereton, Kitchenham, Budgen, & Li, 2008) zoals toegelicht in Bijlage D. Daartoe worden verschillende experts uit het cybersecurity werkveld door middel van semigestructureerde interviews geconsulteerd.

In paragraaf 4.2 wordt kort uiteengezet hoe de planning en het proces van het afnemen van de interviews is verlopen. Hierbij wordt benadrukt welke aandachtspunten bij het uitvoeren van (semigestructureerde) interviews belangrijk zijn en hoe hier invulling aan gegeven is. Vervolgens wordt in paragraaf 4.3 beschreven wat de belemmeringen waren in de uitvoering van het onderzoek, oftewel het zogenaamde veldwerk.

Paragraaf 4.4 beschrijft de risico's per categorie die de experts onderkennen op basis van de gegevens in het ontwikkelde model, waarna in paragraaf 4.5 wordt uitgeweid over de vulling van het model met de gevonden risico's.

4.2. Planning interviews

Te interviewen persoon	Datum gepland	Interview afgenomen	Verslag uitgewerkt
IT-auditor – RE	26-2-2020	26-2-2020	10-3-2020
CEH - Certified Ethical Hacker	27-3-2020	02-4-2020	17-4-2020
CERT - Functionaris	19-4-2020	Niet mogelijk	n.v.t.
CISO - Overheid	27-4-2020	Niet mogelijk	n.v.t.
Hoofd SOC	19-2-2020	19-2-2020	10-3-2020
Security Adviseur en IT-auditor	21-2-2020	21-2-2020	10-3-2020
CISO	02-3-2020	02-3-2020	10-3-2020
Security Analist	Back-up	Niet mogelijk	n.v.t.
CISSP/OSCP	Back-up	Niet mogelijk	n.v.t.
Adviseur Informatiebeveiliging/FG	30-4-2020	25-05-2020	02-06-2020

Na het uitvoeren van de interviews is een data analyse proces (Maimbo & Pervan, 2005) doorlopen om tot de hieronder (zie paragraaf 4.4) beschreven uitkomsten te komen. In Bijlage G is de coderingsmatrix opgenomen welke het data-analyse proces samenvat. In deze matrix wordt van transcript via open code naar gericht coderen een selectie (Strauss & Corbin, 1998) van gevonden risico's getoond.

4.3. Verloop veldwerk

Halverwege het uitvoeren van de interviews zorgden de maatregelen ten aanzien van het COVID-19 virus voor een verstoring in de planning. Ook bleken een aantal respondenten niet meer beschikbaar vanwege COVID-19 beperkingen en/of een verhoogde werkdruk. Dit, in combinatie met een afgebakend tijdsbestek voor het empirische onderzoek, heeft voor een zestal afgenomen interviews gezorgd in plaats van de vooraf geplande acht. Desalniettemin was er toch sprake van een

voldoende mate van verzadiging. Dit bleek uit het feit dat er gedurende de twee laatste interviews slechts kleine nuanceverschillen waren in de antwoorden en er weinig nieuwe informatie naar voren kwam.

Tijdens de interviews bleek het bepalen van risico's voor vijf niveaus voor de experts te fijnmazig. Daarom is er, in overleg met de deskundigen, voor gekozen om het aantal terug te brengen naar drie. Dit om uiteindelijk de toepasbaarheid van het model ten goede te komen.

4.4. Uitkomsten van de interviews

De uitkomsten uit de gehouden interviews resulteren in de beantwoording van de volgende deelvraag: *2.2. Welke risico's zijn te verbinden aan de verschillende niveaus van het ontwikkelde model?*

In de volgende paragrafen worden de uitkomsten van de interviews per categorie en model beschreven, ten einde deze in de conclusie te kunnen toevoegen aan het ontwikkelde model en op die manier antwoord te kunnen geven op de hoofdvraag van dit onderzoek. De specifieke antwoorden zijn terug te vinden in de interview transcripten (Bijlage F) en zijn gegroepeerd in de coderingsmatrix (Bijlage G).

4.4.1. Risicogebieden procesvolwassenheid

Ad-Hoc

Bedrijfscontinuïteit bij incidenten: Uit de interviews blijkt dat alle respondenten aangeven dat de continuïteit van het bedrijf in deze fase het grootste risico vormt. Aangegeven wordt dat het niet beschrijven van de processen en het niet hebben van documentatie kan resulteren in catastrofale schade voor het bedrijf als er iets mis zou gaan.

Geen indicatoren: in de eerste fase van procesvolwassenheid geven de respondenten aan dat het gemis van indicatoren ervoor zorgt dat een bedrijf geen mogelijkheid heeft om incidenten vroegtijdig te onderkennen. Op deze manier heeft een bedrijf voornamelijk "unknown-unknowns", en is zich dus niet bewust van de gevaren die er schuilen, nog dat ze deze begrijpen en er adequaat op kunnen handelen.

Wettelijk aansprakelijk: uit het empirische onderzoek is gebleken dat door de aantoonbare nalatigheid die er vaak plaatsvindt in deze fase een risico is voor juridische gevolgen. De wet schrijft een bepaalde mate van verantwoordelijkheid voor die een bedrijf heeft in het nemen van acties voor goed bestuur en beschermen van haar klanten.

Makkelijk doelwit: ondanks het simplistische karakter wat een bedrijf in deze fase heeft, blijkt uit de interviews dat dit erin resulteert dat het bedrijf een makkelijk doelwit kan worden voor kwaadwillende door de beperkte mate van scheiding van taken en verantwoordelijkheden.

De medewerker: op het laagste niveau van procesvolwassenheid merken de respondenten op dat de meeste waarde van het bedrijf ligt bij de medewerkers. De mens is vaak een onmisbare factor, waarbij er weinig wordt gedaan om het eventuele verlies hiervan op te kunnen vangen. Hierdoor is de kennis van aanwezige processen en systemen dus zeer kwetsbaar indien er iets zou gebeuren met een medewerker.

Onnodige kosten op lange termijn: als laatste geven alle respondenten nog aan dat in de Ad-Hoc fase er vaak gekozen wordt voor de korte termijn, goedkoopste oplossing die op de lange duur vaak niet de voordeligste optie blijkt. Daarnaast zijn dit ook vaak oplossingen die gekozen worden voor

een direct probleem en niet bijdragen aan het grotere geheel. Hierdoor zijn er regelmatig extra investeringen nodig op de lange duur, om deze oplossingen te integreren in de bedrijfssystematiek.

Moderate (Engaged / Structured / Managed)

Glijdende schaal: unaniem kwam tijdens het onderzoek naar voren dat de ondervraagde experts aangaven dat alle benoemde risico's in meer of mindere mate aanwezig zijn naarmate een organisatie stijgt en/of daalt in haar volwassenheidsniveau. Vandaar dat dit op een manier wordt geïmplementeerd in het raamwerk.

Afhankelijkheid van anderen stijgt: naar mate de volwassenheid van het bedrijf stijgt is het ook aannemelijk dat er meer connecties ontstaan met externen. Dit zijn afhankelijkheden waar het bedrijf geen, of in zeer beperkte mate, controle over heeft.

Connecties zijn onbekend: door het geleidelijk volwassen worden van een bedrijf zullen er koppelingen ontstaan die niet voor iedereen duidelijk zijn. Eén van de respondenten merkte op dat dit er bij verschillende bedrijven voor gezorgd heeft dat het doorvoeren van wijzigingen op de processen storingen tot gevolg had die niet vooraf voorzien waren.

Scheefgroei in organisatieontwikkeling: het groeien in volwassenheid van een bedrijf gebeurt op meerdere vlakken, de respondenten gaven aan dat er altijd een bepaalde mate van scheefgroei plaatsvindt tussen deze vlakken. Vanwege de verschillen in complexiteit om te groeien op deze vlakken is het mogelijk dat er een buitensporig ongelijke groei ontstaat waarbij er nieuwe, niet voorziene risico's worden geïntroduceerd.

Toenemende complexiteit: het onderzoek wijst uit dat met het stijgen van de volwassenheid van een organisatie ook de complexiteit toeneemt van de processen, en daarmee de noodzaak dit goed te controleren. Naarmate de volwassenheid toeneemt stijgen ook vaak de koppelingen en daarmee worden nieuwe risico's geïntroduceerd op andere gebieden.

Optimized

Afhankelijkheid van externen: Het empirische onderzoek laat naar voren komen dat in het hoogste niveau van procesvolwassenheid er ook een hoge mate van verbondenheid is met externe partijen. In het huidige tijdperk van sub-leveranciers en diverse serviceproviders wordt de afhankelijk van partijen waar het bedrijf geen controle over heeft steeds hoger. Deze afhankelijkheid kan een risico zijn indien deze verbondenheid niet goed geborgd en afgestemd is.

Verkeerde bedrijfsdoelstellingen: een tweede risico wat de respondenten benoemen is het doorslaan in het volwassenheidsniveau, hierbij wordt aangegeven dat een bedrijf zich te veel focust op optimalisatieslagen en randzaken. Dit kan onbedoeld een "pervers effect" creëren. Door deze shift in focus kunnen de basisprincipes van het bedrijf uit het zicht verloren raken en dit kan resulteren in het verkwisten van bedrijfsassets.

Hoge overhead kosten: In de zoektocht naar maximale procesvolwassenheid laat het empirische onderzoek zien dat dit bij veel bedrijven resulteert in exponentieel hogere overheadkosten zonder de bijbehorende gelijkwaardige groei van omzet en/of winst.

Schijnveiligheid: het optimaliseren van de processen kan een bedrijf het gevoel geven van "alles in de hand hebben". Dit is in een wereld van verbondenheid en afhankelijkheden niet mogelijk, maar deze fase kan een bedrijf het valse gevoel van veiligheid kunnen geven en suggereren dat alle risico's inzichtelijk zijn. Het onderzoek merkt op dat er nooit een mate van gelatenheid mag ontstaan ten opzichte van de risico's voor het bedrijf.

Verminderde flexibiliteit: Het groeien in procesvolwassenheid staat inherent aan het complexer en uitgebreider worden van de aanwezige processen. Daarnaast zijn er ook meer stappen die doorlopen moeten worden en zijn deze stappen ook meer rigide vergeleken met lagere volwassenheidsniveaus. De interviews laten naar voren komen dat dit gepaard gaat met een minder flexibele organisatie, waarbij ook het aanpassingsvermogen van het bedrijf vermindert. Een bedrijf kan in deze fase ook minder makkelijk innovaties en veranderingen doorvoeren.

4.4.2. Risicogebieden digitalisatie

Ad-Hoc

Onnodige kosten: zonder een gedegen visie en plan aangaande de aanschaf van hard en software ontstaat er een functionaliteitsverlies en een grote kans op de aanwezigheid van “Shadow-IT”. Deze losstaande IT-middelen zorgen voor een optimalisatie verlies en dit genereert vrijwel altijd onnodige kosten.

Kwetsbaar voor simpele aanvallen: door het zonder een doordacht plan IT-middelen bij de organisatie naar binnen te halen, introduceert men een steeds grotere vatbaarheid voor de meeste basis aanvallen die kwaadwillende kunnen uitvoeren. Het niet beperken van middelen en rechten zorgt er tevens voor dat een aanvaller ook niet beperkt wordt in zijn mogelijkheden, blijkt uit de antwoorden van de respondenten.

Geen indicatie op incidenten: het empirische onderzoek laat zien dat op het laagste niveau van digitalisatie er geen ruimte en mogelijkheden zijn om te meten wat de bedrijfssystemen doen. Dit zorgt er vervolgens voor dat er geen mogelijkheid is om vroegtijdig problemen en/of falen van systemen te onderkennen. Een bedrijf zal in deze fase snel verrast worden door een incident in de digitalisatie.

Bedrijfscontinuïteit in gevaar: de interviews geven weer dat in deze fase van digitalisatie er geen rekening gehouden wordt met het uitvallen van middelen of de personen die cruciaal zijn voor de inzet hiervan. Dit resulteert bij uitval van een van deze factoren direct in het stoppen van bedrijf kritische processen en brengt daarmee de voorzetting van het bedrijf in gevaar.

Efficiëntie beperkingen: op dit niveau van digitalisatie mist de kennis binnen het bedrijf om de juiste middelen te kiezen en/of deze op de juiste manier in te zetten. Hieruit komt naar voren dat dit een verlies van efficiëntie te weeg brengt en daardoor de optimalisatie van de organisatie in gevaar brengt.

Mens als risico factor: een van de geïnterviewden benadrukte ook het aspect van de mens in deze fase van digitalisatie. Op dit niveau is de mens nog vaak de verbindende schakel en de IT in meer of mindere mate uitbesteed.

Moderate (Engaged / Structured / Managed)

Glijdende schaal: ook in deze categorie kwam unaniem naar voren dat de ondervraagde experts aangaven dat alle benoemde risico’s in meer of mindere mate aanwezig zijn naarmate een organisatie stijgt en/of daalt in haar volwassenheidsniveau.

Complexiteit neemt toe: het verhogen van de mate van digitalisatie staat gelijk aan het verhogen van de complexiteit ervan. Gedurende het proces van automatiseren worden er steeds meer middelen gekoppeld, dit is een exponentiele uitbreiding van mogelijkheden maar ook van het aantal gegevensstromen. Het inzicht houden in de digitale voetprint wordt naarmate deze stijgt steeds complexer.

Kennis als knelpunt: het uitbreiden van de digitale mogelijkheden van een bedrijf en daarmee, zoals in het vorige risico benoemd, de hogere mate van complexiteit vraagt om specifieke kennis. Naarmate de mate van digitalisatie toeneemt zal het in huis hebben van voldoende (specialistische) kennis steeds moeilijker worden.

Introductie van nieuwe risico's: ook in deze categorie herhalen de respondenten nogmaals de kans op scheefgroei in het volwassenheidsniveau en de bijbehorende risico's. Door deze onevenredige groei kunnen er onbedoeld nieuwe kwetsbaarheden worden geïntroduceerd. Veelal zal de introductie van nieuwe hardware makkelijker gaan dan het verhogen van het kennisniveau wat voor het gebruik noodzakelijk is.

Afhankelijkheden stijgen: door een steeds hogere mate van digitalisatie neemt ook de mate van afhankelijkheid van leveranciers en dienstverleners toe. Uit de interviews komt naar voren dat MKB'ers veelal externe partijen/expertise nodig hebben om automatiseren door te voeren en te onderhouden. Hierdoor is de afhankelijkheid van deze partijen en het moeten vertrouwen daarop in steeds grotere mate aanwezig naarmate het volwassenheidsniveau stijgt in deze categorie.

Optimized

Hoge afhankelijkheid van externen: uit het empirische onderzoek blijkt dat bedrijven bij het bereiken van het hoogste volwassenheidsniveau een hoge verbondenheid hebben met leveranciers en dienstverleners. Hierdoor wordt ook de mate van controle die zij hebben over het hele digitale landschap waar zij zich in bevinden beperkt. Het risico op "Vendor Lock-in" is in dit stadium ook een aspect waarvoor gewaakt moet worden, maar wat niet altijd voorkomen kan worden.

Hoge mate van complexiteit: het verhogen van de mate van automatisering is inherent aan de complexiteit van het digitale landschap van een organisatie. Hierdoor wordt het steeds lastiger om wijzigingen door te voeren en de kennis en kunde in huis te hebben om het beheer van het digitale speelveld uit te voeren.

Single Point of Failure (SPOF): de volledige connectiviteit tussen alle bedrijfsprocessen en het automatiseren hiervan brengt het risico met zich mee dat een enkel incident alle gekoppelde processen zou kunnen raken. Dit stadium kan er dus, door zijn grote mate van verbondenheid, onbedoeld voor zorgen dat een enkele storing het hele bedrijfssysteem platlegt.

Nieuwe risico's worden geïntroduceerd: het continue volgen van de laatste trends op digitaal gebied, de verbondenheid tussen alle systemen binnen het bedrijf en de steeds grotere mate van virtualisatie toepassingen vergroot niet alleen de mogelijkheden maar introduceert ook continue nieuwe mogelijkheden voor kwaadwillende. Zonder bewust te zijn steeds meer gevaar te lopen.

Hoge kosten: de respondenten geven aan dat het voor een bedrijf zeer hoge kosten met zich meebrengt om dit niveau van digitalisatie te bereiken. De kans is zeer groot dat dit streven een mismatch tussen kosten en baten oplevert en daardoor zijn doel voorbijstreeft.

Doel op zich: het onderzoek geeft ook weer dat het streven naar de hoogste mate van digitalisatie een doel op zich kan worden en daarmee het beoogde effect van het verbeteren van de bedrijfsvoering voorbijstreeft.

4.4.3. Risicogebieden cyberweerbaarheidsmaatregelen

Initial

Geen detectie: in dit stadium laat het onderzoek duidelijk zien dat er geen enkele mogelijkheid is tot het herkennen van bedreigingen op de bedrijfssystemen. Er kan niet gecontroleerd worden wat er

binnenkomt en vervolgens is er ook geen mogelijkheid tot het onderkennen van vreemde gedragingen van de aanwezige hard- en software.

Geen herstel: indien er ook maar iets gebeurt met bedrijfssystemen, door een fout of door een kwaadwillende, is het onmogelijk om te herstellen. Zonder een basis vorm van herstelsystematiek kan zelfs een klein incident catastrofaal zijn voor de organisatie omdat er geen herstelpunt gedefinieerd is van waaruit dit plaats moet vinden.

Hoge kwetsbaarheid: het laagste niveau van cyberweerbaarheidsmaatregelen zorgt ervoor dat het bedrijf kwetsbaar is voor de meest simpele aanvallen en zelfs geautomatiseerde acties tegen bedrijfsassets uitgevoerd kunnen worden. In deze fase heeft een bedrijf geen enkele verdediging in huis.

Juridische aansprakelijkheid: bij dit benoemde risico komen de termen “due diligence” en “due care” naar voren. Dit betekend dat een bedrijf wettelijk kan worden aangerekend dat zij niet minimale maatregelen hebben genomen om zich (en hun klanten) te beschermen tegen incidenten die het bedrijf had kunnen voorzien.

IT als grootste kwetsbaarheid: Het onderzoek wijst uit dat in deze fase alle aanwezige IT kan worden misbruikt door een aanvaller en daardoor ook de grootste risico factor is voor het bedrijf.

Moderate (Basic / Capable / Efficiency)

Glijdende schaal: ook in deze laatste categorie kwam unaniem naar voren dat de ondervraagde experts aangaven dat alle benoemde risico’s in meer of mindere mate aanwezig zijn naarmate een organisatie stijgt en/of daalt in haar volwassenheidsniveau.

Weerstand: het empirische onderzoekt wijst uit dat de implementatie van weerbaarheidsmaatregelen vaak lijdt tot weerstand vanuit de organisatie. Dit kan zijn omdat de maatregelen beperkingen opleggen of omdat het wordt geïnterpreteerd als een teken van wantrouwen.

Efficiëntie beperkingen: zoals ook al bij bovenstaand risico benoemd kunnen ingevoerde maatregelen restricties opwerpen, deze restricties zorgen voor minder flexibiliteit en mogelijkheden. Dit kan, ondanks een hogere mate van veiligheid, de productie van het bedrijf schaden door handelingssnelheid te verkleinen.

Vatbaar voor complexere aanvallen: ondanks een bepaalde mate van genomen maatregelen blijft een bedrijf in deze fases vatbaar voor de wat complexere aanvallen. Het volledig voorkomen van incidenten of de gevolgen hiervan is niet mogelijk.

Optimizing

Gebruiksvriendelijkheid neemt af: in de hoogste mate van genomen cyberweerbaarheidsmaatregelen is de kans op het beperken van de gebruiksvriendelijkheid dermate hoog dat het voor onwerkbare situaties kan zorgen. Security moet altijd ondersteunen aan de inzetbaarheid van systemen en niet de bedrijfsvoering dermate hinderen dat het niet meer werkbaar wordt, geven de respondenten aan.

Schijnveiligheid: de hoogste mate van genomen weerbaarheidsmaatregelen geeft de illusie dat alle risico’s zijn afgedekt. Er zullen altijd onvoorziene risico’s zijn en er worden continue nieuwe kwetsbaarheden ontdekt. In deze fase moet een organisatie waken voor een vals gevoel van veiligheid.

Zeer hoge kosten: kosten en baten moeten altijd in verhouding met elkaar zijn, door het hoogste niveau te ambiëren is het scheefgroeien in de verhouding tussen beide factoren zeer groot. Veel weerbaarheidsmaatregelen zijn prijzig om goed te implementeren en actueel te houden, dit moet wel in verhouding tot de te beschermen belangen staan.

Cybermoeheid: de respondenten geven aan dat bedrijven die een uitermate hoge mate van weerbaarheidsmaatregelen nastreven de kans lopen om cybermoeheid onder haar medewerkers te creëren. Door het doorslaan in de beveiliging kunnen medewerkers uit het oog verloren worden en kunnen zij zich achtergesteld of zelfs gewantrouwd voelen. Dit kan ervoor zorgen dat medewerkers bewust om de geïmplementeerde systemen heen gaan.

Hoge mate van complexiteit: het hoogste niveau bereiken en behouden is een zeer complex proces en is ook zeer afhankelijk van de aanwezige kennis bij de personen die het moeten beheren.

4.4.4. Overige niet gecategoriseerde risico's

Naast de risico's die benoemd zijn door de verschillende respondenten zijn er ook een aantal niet aan specifieke categorieën gehangen risico's gedefinieerd. Deze zullen waar mogelijk, in samenhang met de theorie, worden toegevoegd aan het model.

Verantwoordelijkheid afschuiven: Het empirische onderzoek brengt veelvuldig naar voren dat, met de verschuiving naar clouddiensten en serviceproviders er ook een tendens is met betrekking tot het afschuiven van verantwoordelijkheden.

Verkeerde risico inschatting: de respondenten geven aan dat veel bedrijven de risico's van cyber incidenten nog niet goed kunnen inschatten. Veelal zien zij een incident bij een andere partij niet als een potentieel risico voor hun eigen onderneming. Zeker in geval van cyber zijn halve maatregelen niet voldoende en is het nodig het principe van "Cyber in Depth" te volgen.

Kwetsbaarheid: de gemiddelde MKB'er is uitermate kwetsbaar voor incidenten. Dit komt ook vanwege het feit dat een aanvaller maar één opening nodig heeft om binnen te komen en de verdedigende partij (de MKB'er) moet proberen alles tegen te houden.

Cybersecurityniveau: de geïnterviewden geven aan dat cyber risico's en organisatie risico's onlosmakelijk met elkaar verbonden zijn. Hoe meer een organisatie aan de uitersten van een volwassenheidsschaal ten opzichte van proces en digitalisatie zit, des te groter is de impact voor de bedrijfsvoering als er een incident plaatsvindt.

4.5. Complementeren van het ontwikkelde model

Alle gevonden risico's zijn door middel van codering opgenomen in de coderingsmatrix (Bijlage G), vervolgens zijn alle antwoorden van alle respondenten gefilterd per categorie en niveau. Per categorie en niveau zijn de codes samengevoegd tot vijf à tien bruto risico's. Deze zijn vervolgens allemaal ingevuld op het voorlopige model (Bijlage A) waarbij risico's die zowel in procesvolwassenheid als ook in mate van digitalisatie naar voren kwamen zijn samengevoegd. Daarna zijn de restrisico's van genomen cyberweerbaarheidsmaatregelen afgezet tegen de risico's uit de andere twee constructen. In sommige gevallen zorgden de wel genomen maatregelen voor het opheffen van de risico's uit de eerste twee constructen, en in andere gevallen zorgde een gebrek aan genomen maatregelen voor het introduceren van extra risico's.

Vervolgens zijn de risico's vergeleken met de karaktereigenschappen van de drie categorieën (procesvolwassenheid, digitalisatie en cyberweerbaarheidsmaatregelen) en zijn de risico's

weggestreept die op basis van deze karaktereigenschappen niet voldoen aan de omschrijving van een MKB'er in deze fase zoals gegeven in de verschillende volwassenheid matrixen (Bijlage B). De niet gecategoriseerde risico's zijn gebruikt in het proces van wegstrepen en hebben bijgedragen aan de keuze van de specifieke netto risico's. Dit alles is zichtbaar in het definitieve model voor validatie (Bijlage C1).

Vervolgens is er als validatieslag nogmaals contact opgenomen met de respondenten (Bijlage H) en hen verzocht het voltooide model te beoordelen op een aantal punten en deze aanvullingen zijn vervolgens opgenomen in een overzicht (Bijlage I. Uitkomst validatie respondenten). Het definitieve model is vervolgens tegen het licht gehouden en nog verder aangescherpt middels deze validatieslag en gevisualiseerd in het definitieve model na validatie (Bijlage C2). Een groot deel van de op- en aanmerkingen is meegenomen in het herziene model. De tip voor het vervaardigen van een model dat bestaat uit afbeeldingen en minder opsommingen is een goede aanvulling indien het model in een awareness campagne ingezet zou worden.

5. Discussie, conclusies en aanbevelingen

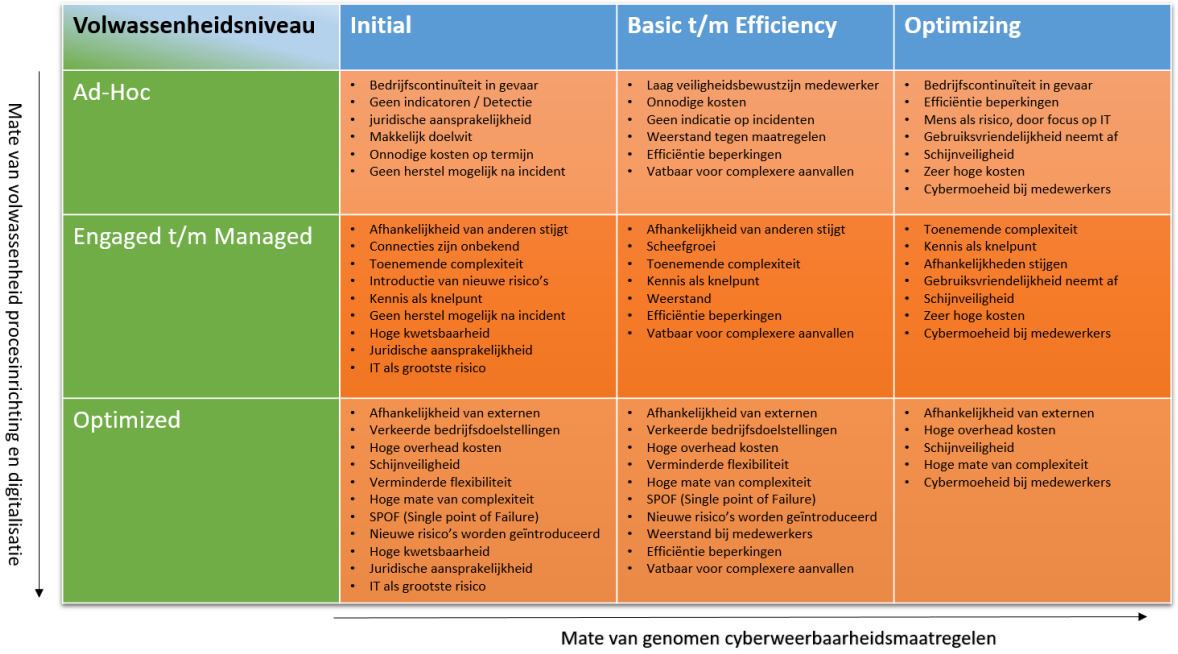
5.1. Conclusies

Om tot een uiteindelijk antwoord op de hoofdvraag te komen en dus een gevuld model te formuleren is een beantwoording van de deelvragen noodzakelijk. Deze zullen puntsgewijs hieronder worden samengevat.

1. *Hoe is het ontwikkelde model toe te passen op een MKB-organisatie?*
   In het literatuuronderzoek is per categorie het meest passende model geselecteerd op basis van zijn karakteristieken. Voor elk van deze modellen is een beoordelingsmatrix ontwikkeld (zie Bijlage B) om het specifieke niveau van het bedrijf op elk van de categorieën te bepalen. Aan de hand van drie niveaubepalingen kan het risicomodel worden geraadpleegd. De gekozen karakteristieken zijn gebruikt om de specifieke risico's te selecteren die van toepassing zijn voor het niveau.
2. *Welke risico's zijn te verbinden aan de verschillende niveaus van het ontwikkelde model?*
   De gevonden risico's zijn zeer afhankelijk van het specifieke volwassenheidsniveaus van een organisatie. Het is gebleken dat de risico's die gekoppeld zijn aan de uiterste volwassenheidsniveaus eerder te omschrijven zijn als bedrijfsrisico's dan als specifieke cyberrisico's. Dit geeft aan dat het niet nemen van de juiste maatregelen grote impact kan hebben op het voortbestaan van een MKB-organisatie. De risico's die hieruit voortkomen zijn te wijten aan de gevolgen van cyber-incidenten, maar gaan verder dan het niveau van cyberrisico's. Daarbij heeft het onderzoek aangetoond dat aan de uiterste waarden van een volwassenheidsschaal duidelijke risico's gekoppeld kunnen worden, maar daarbinnen wordt het minder stringent. Dit is in het uiteindelijke model gevisualiseerd door het samenvoegen van de middelste schalen.
3. *Op welke manier is de validiteit van het model te meten?*
   De validiteit van het model is op twee manieren gemeten. Allereerst door in de praktijk te toetsen of de ontwikkelde matrixen een daadwerkelijke graadmeter vormen voor volwassenheid binnen het MKB. Hiervoor is een selectie gemaakt van volwassenheidsmodellen gericht op het MKB, aangezien de meeste zijn ontwikkeld voor grote organisaties. Ten tweede is de validiteit van het ontwikkelde model gemeten via twee methodes: door het model bij verschillende MKB'ers te doorlopen, en daarnaast door te toetsen of het model een juiste risico-indicator zou zijn geweest voor MKB'ers die in het verleden slachtoffer zijn geworden van een cyber incident.

De beantwoording van de deelvragen en de gepresenteerde risico's in hoofdstuk 4 hebben geleid tot het antwoord op de hoofdvraag *"Hoe ziet een raamwerk eruit waarmee een MKB-ondernemer inzichtelijk krijgt welke risico's hij loopt voor zijn bedrijfsvoering, vanwege onvoldoende genomen cyberweerbaarheidsmaatregelen?".*

Het onderzoek heeft geresulteerd in onderstaand model en is geschikt voor het MKB. Het model toont op basis van de verschillende volwassenheidsniveaus overzichtelijk de grootste risico's voor het bedrijf in relatie tot de genomen cyberweerbaarheidsmaatregelen.



Definitief Model (Zie ook Bijlage C2): risico's voor bedrijfsvoering voor wat betreft cybersecurity

5.2. Discussie – reflectie

Uit het onderzoek kwam al snel naar voren dat het veronderstelde aantal niveaus van vijf te specifiek bleek. Gedurende de interviews werd steeds weer herhaald dat de tussenliggende niveaus een dusdanige mate van interpretatie mogelijk maakte, dat ervoor is gekozen om de interviews aan te passen en uiteindelijk ook het definitieve model.

Daarbij had ik de verwachting dat er meer technische risico's uit de interviews naar voren zouden komen. Echter, ondanks de diversiteit van de geïnterviewden (van pentester t/m managementniveau) bleek herhaaldelijk dat de bedrijfsvoering risico's meer van belang zijn, en de technische aspecten een achterliggende oorzaak zijn.

Ondanks het gelimiteerde aantal afgenomen interviews vanwege afzeggingen in verband met Covid-19 is toch een redelijke mate van verzadiging in de antwoorden behaald. De lange duur van de interviews (meer dan twee uur) maakte het lastig om deze te plannen of via beeldbellen uit te voeren. Beeldbellen werd tevens door respondenten afgeraden bij semigestructureerde interviews en is om die reden ook niet toegepast.

Ondanks de zeer uiteenlopende kennis en ervaring van de respondenten werd in de interviews niet afgeweken van de vooraf bepaalde structuur. Door het gebruiken van het raamwerk (en deze vooraf aan de respondenten toe te zenden) konden alle vragen beantwoord worden tijdens het empirische onderzoek. De vooraf bedachte toetsing van de risico's door middel van de Mitre ATT&CK matrix heeft achteraf toch niet het gewenste effect opgeleverd omdat dit te diep op de techniek in gaat en de risico's op bedrijfsvoering vlak liggen. Een vertaalslag naar specifiek technische risico's zou wel meerwaarde kunnen opleveren voor de bruikbaarheid van het model. Voor een vervolgonderzoek zou een validatieslag op het model uitgevoerd kunnen worden met een andere groep experts.

De betrouwbaarheid is gedurende het onderzoek bewaakt door de transcripten met de respondenten door te nemen op eventuele interpretatie verschillen. Daarnaast heeft het vooraf delen van de matrixen er ook toe geleid dat de antwoorden van de respondenten minder afhankelijk

waren van het uitleggende vermogen van de interviewer. De omstandigheden tijdens het onderzoek hebben er wel voor gezorgd dat de diversiteit van de respondenten kleiner was dan vooraf gepland. De vulling van het model is uiteindelijk wel een gedeeltelijke interpretatie van de onderzoeker en dat zou voor toekomstig gebruik nog eens voorgelegd kunnen worden aan een andere groep van experts. Als validatie is er nog wel een controle slag door de respondenten uitgevoerd op het ontwikkelde model.

Als ik terugkijk op het proces van afstuderen kan ik heel duidelijk stellen dat het halverwege wisselen van functie niet altijd de focus bij het afstuderen heeft gehouden. Daarentegen heeft het onderzoeksonderwerp wel altijd mijn interesse gehouden (en dat doet het nog steeds). Dat zorgde er gedurende het afstudeerproces voor dat ik nooit moeite had om me er weer voor in te zetten. Dit was een zeer prettige verandering ten opzichte van mijn Bachelor thesis ruim tien jaar geleden. Naarmate het empirische deel vorderde merkte ik ook dat ik steeds meer plezier ging krijgen in het uitvoeren van de interviews, maar er wel voor moest blijven waken niet in (interessante) discussies te verzanden. Achteraf had ik de interviews wel iets dichter achter elkaar willen plannen om de vaart erin te houden, maar dit was ook niet helemaal mogelijk geweest met Covid-19.

Kijkende naar de toekomst (en eigenlijk ook een beetje naar het verleden) heeft het uitgevoerde onderzoek ervoor gezorgd dat ik mijn huidige baan als informatie beveiliger ben gaan ambiëren en gelukkig deze ook heb kunnen bemachtigen. Ik heb mede door mijn Masterstudie en deze thesis in het bijzonder mijn richting voor de rest van mijn carrière gevonden.

5.3. Aanbevelingen voor de praktijk

Het ontwikkelde model kan, door het in de praktijk toe te passen, een MKB'er voorzien van de juiste focus van zijn kostbare assets. Het inzicht krijgen in de risico's die je als bedrijf loopt zijn cruciaal om de juiste beslissingen te kunnen nemen.

5.4. Aanbevelingen voor verder onderzoek

Dit onderzoek heeft te allen tijde het doel gehad een model te ontwikkelen wat generiek is voor het MKB. Dit betekend dat er een hoop zaken buiten scope zijn gebleven, waaronder de sector waar de MKB'er zich in bevindt. Tijdens veel van de interviews is dit ook ter sprake gekomen, een aannemer met 50 medewerkers is toch echt iets anders dan een clouddiensten leverancier met 200 techneuten of een psychologiepraktijk met 10 behandelaren. Het verdient dan ook de aanbeveling om voor vervolgonderzoek te kijken of er een verdiepingsslag gemaakt kan worden op het ontwikkelde model specifiek voor een bepaalde sector. Op deze wijze kan de toepasbaarheid nog verder vergroot worden. Daarnaast is het principe van "weten wie je vijanden zijn" een interessant aspect wat niet is meegenomen in de scope van dit onderzoek, maar dit zou wel bepaalde keuzes kunnen beïnvloeden.

Referenties

Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. *Computer Science & Information Technology, 51*.

Ashrafi, N., & Kuilboer, J.-P. (2001). Managing network security. *Managing information technology in a global economy*, 122-124.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering, 1*(3), 213-222. doi:10.1007/s12599-009-0044-5

Brereton, P., Kitchenham, B., Budgen, D., & Li, Z. (2008). *Using a protocol template for case study planning.* Paper presented at the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12.

Buecker, A., Borrett, M., Lorenz, C., & Powers, C. (2010). Introducing the IBM security framework and IBM security blueprint to realize business-driven security. *IBM Redpaper, 4528*(1), 1-96.

Butkovic, M. J., & Caralli, R. A. (2018). *Advancing Cybersecurity Capability Measurement Using the CERT ® -RMM Maturity Indicator Level Scale*. Retrieved from

Castelli, C., Gabriel, B., Yates, J., & Booth, P. (2018). Strengthening digital society against cyber shocks: Key findings from The Global State of Information Security® Survey 2018. *The Global State of Information Security® Survey 2018*. Retrieved from https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf

Chabinsky, S. (2013). Cyber security for SMEs: prioritize, isolate and protect. *50*(7), 30.

Chen, Y.-Y. K., Jaw, Y.-L., & Wu, B.-L. (2016). Effect of digital transformation on organisational performance of SMEs. *Internet Research, 26*(1), 186-212. doi:10.1108/IntR-12-2013-0265

Cybenko, G. (2014). TIM Lecture Series Cybersecurity Metrics and Simulation. *Technology Innovation Management Review*. Retrieved from https://timreview.ca/sites/default/files/article_PDF/TIMLS_Cybenko_TIMReview_October2014.pdf

de Bruin, R., & von Solms, S. H. (2015). *Modelling Cyber Security Governance Maturity*.

De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management, 26*(2), 123-137.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307-324.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats*: Apress.

Dreher, N., & Dreher, H. (2011). Empowering doctoral candidates in finding relevant concepts in a literature set. *The International Journal of Doctoral Studies, 6*, 33-49.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security, 13*(4), 297-310. doi:10.1108/09685220510614425

Hamidi, S. R., Aziz, A. A., Shuhidan, S. M., Aziz, A. A., & Mokhsin, M. (2018). *SMEs maturity model assessment of IR4. 0 digital transformation.* Paper presented at the International Conference on Kansei Engineering & Emotion Research.

Hammer, M. (2007). The process audit. *Harvard business review, 85*(4), 111.

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM systems journal, 38*(2.3), 472-484.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly, 28*(1), 75-105.

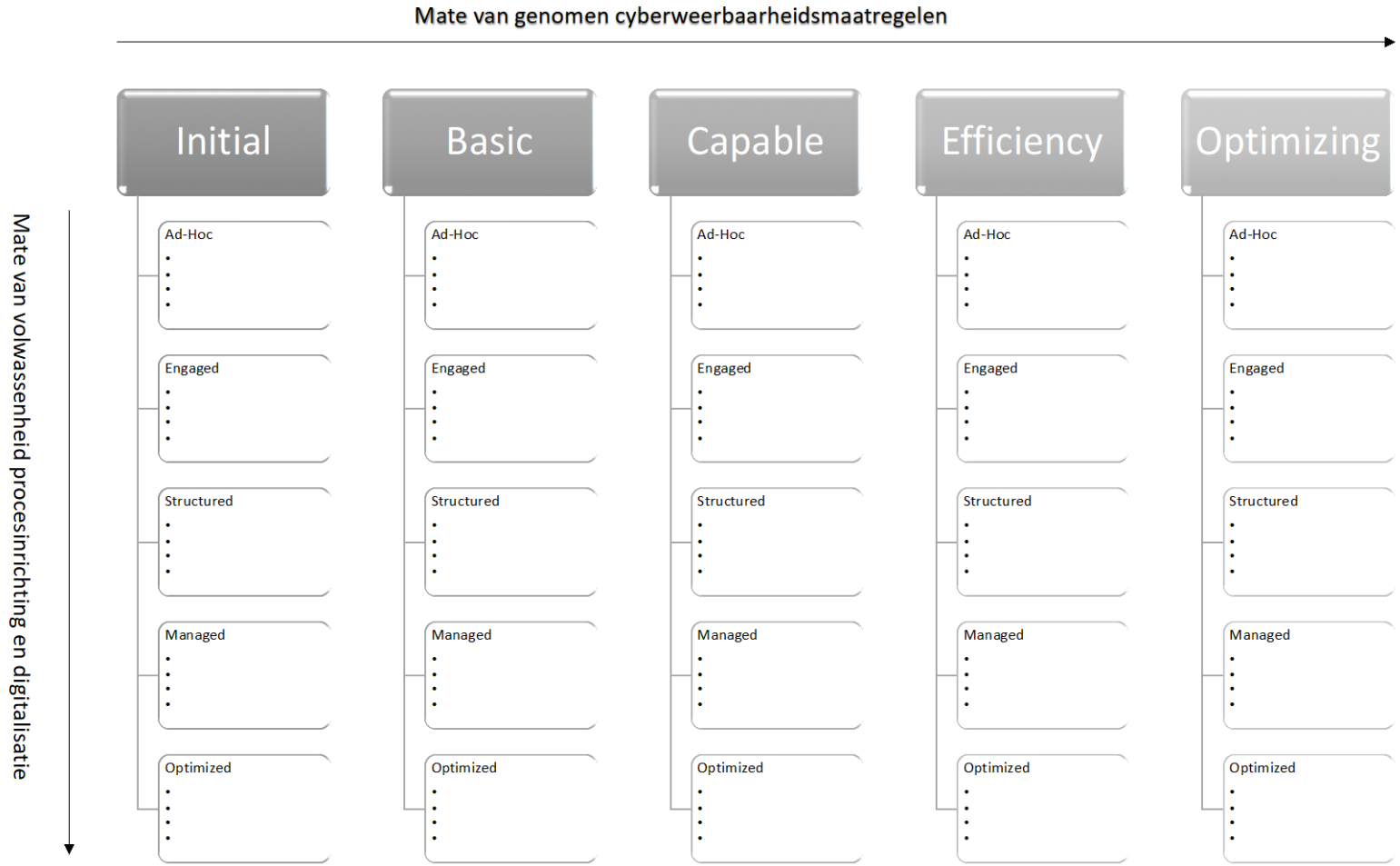
Hribar Rajterič, I. (2010). Overview of Business Intelligence Maturity Models. *Management : Journal of Contemporary Management Issues, 15*(1).
Humphrey, W. S. (1988). Characterizing the software process: a maturity framework. *IEEE Software, 5*(2), 73-79. doi:10.1109/52.2014
Industry, S. (2018). Cyber Security Scan. Retrieved from https://smartindustry.nl/ondersteuning/cyber-security-scan/
Initiative, J. T. F. T. (2012). SP 800-30. Managing Information Security Risk: Guide for Conducting Risk Assessments. *NIST Special Publication*.
Jeston, J. (2014). *Business process management*: Routledge.
Jong, B. d. (2017). Ook Nederland bedreigd door wereldwijde gijzeling computer *Algemeen Dagblad*. Retrieved from https://www.ad.nl/buitenland/ook-nederland-bedreigd-door-wereldwijde-gijzeling-computer~a336d6fb/
Justitie, M. v. (2019). Cybercrime. Retrieved from https://www.politie.nl/themas/cybercrime.html
Kotarba, M. (2017). Measuring digitalization–key metrics. *Foundations of Management, 9*(1), 123-138.
Le, N. T., & Hoang, D. B. (2016, 2016). *Can maturity models support cyber security?*
Lim, C. (2010). *Risk Management in Small-medium Enterprises (SMEs): How does Risk Management in Small-medium Enterprise (SMEs) contribute to the Company's Financial Performance?* : GRIN Publishing.
Maimbo, H., & Pervan, G. J. P. P. (2005). Designing a case study protocol for application in IS research. 106.
Miles, M. B., Huberman, A. M., Huberman, M. A., & Huberman, M. (1994). *Qualitative data analysis: An expanded sourcebook*: sage.
MITRE ATT&CK MATRIX. (2020). Retrieved from https://attack.mitre.org/matrices/enterprise/
Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine, 151*(4), 264-269.
Müller, A., von Thienen, L., & Schröder, H. (2004). *IT-Controlling: So messen Sie den Beitrag der Informationstechnologie zum Unternehmenserfolg*. Retrieved from
NCSC. (2020). Vele Nederlandse Citrix-servers kwetsbaar voor aanvallen. Retrieved from https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen
NCSC. (2021). Gevolgen van Microsoft Exchange kwetsbaarheden groot voor Nederlandse organisaties en bedrijven. Retrieved from https://www.ncsc.nl/actueel/nieuws/2021/maart/16/schade-microsoft-exchange
NOREA. (2015). Handreiking Cybersecurity Assessment. In *NOREA* (pp. 17).
Osborn, E. (2015). Business versus technology: Sources of the perceived lack of cyber security in SMEs.
Paulk, M. C., Weber, C. V., Curtis, B., & Chrissis, M. B. (1995). *The capability maturity model: Guidelines for improving the software process* (Vol. 441): Addison-wesley Reading, MA.
Purdy, G. (2010). ISO 31000:2009—Setting a New Standard for Risk Management. *Risk analysis, 30*(6), 881-886. doi:10.1111/j.1539-6924.2010.01442.x
PVO, & Brightlands. (2018). Cyberweerbaarheid in Limburg: Samen de waakzaamheid en zelfredzaamheid van het MKB opbouwen en vasthouden. *PVO Platform veilig ondernemen Limburg*
Rea-Guaman, A., Sánchez-García, I., San Feliu, T., & Calvo-Manzano, J. (2017). *Maturity models in cybersecurity: a systematic review.* Paper presented at the 2017 12th Iberian Conference on Information Systems and Technologies (CISTI).
Reulink, N., & Lindeman, L. (2005). Kwalitatief onderzoek. *Participerende observatie, interviewen*.

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal, 18*(2), 328-346. doi:10.1108/14637151211225225
Rohloff, M. (2011). Advances in business process management implementation based on a maturity assessment and best practice exchange. *Information Systems and e-Business Management, 9*(3), 383-403. doi:10.1007/s10257-010-0137-1
Rosenberg, J. M. (2018). Small businesses vulnerable to cyberattacks, then don't act. *PHYS.org*. Retrieved from https://phys.org/news/2018-06-small-businesses-vulnerable-cyberattacks-dont.html
Saunders, M., Lewis, P., & Thornhill, A. (2016). Research methods for Business Students.
Strauss, A., & Corbin, J. (1998). *Basics of qualitative research techniques*: Sage publications Thousand Oaks, CA.
Strupczewski, G. (2021). Defining cyber risk. *Safety science, 135*. doi:10.1016/j.ssci.2020.105143
Tarhan, A., Turetken, O., & Reijers, H. A. (2016). Business process maturity models: A systematic literature review. *Information and Software Technology, 75*, 122-134. doi:10.1016/j.infsof.2016.01.010
Tim Grance, J. H., Marc Stevens, Kristofer O'Neal, Nadya Bartol. (2003). SP 800-35. Guide to Information Technology Security Services. *NIST Special Publication, 800-35*.
Trim, P., & Lee, Y.-I. (2016). *Cyber security management: a governance, risk and compliance framework*: Routledge.
van der Voordt, T. (1998). Methoden en Technieken van Onderzoek.
Van Looy, A., De Backer, M., Poels, G., & Snoeck, M. (2013). Choosing the right business process maturity model. *Information & Management, 50*(7), 466-488. doi:10.1016/j.im.2013.06.002
Verschuren, P., & Doorewaard, H. (2007). Het ontwerpen van een onderzoek. In: Designing a research project](Den Haag 2007). III.
VO-raad. (2013). Handboek Risicomanagement. 27.
Weill, P., & Ross, J. W. (2009). *IT savvy: What top executives must know to go from pain to gain*: Harvard Business Press.
Wester, F. P. J., & Peters, V. A. M. (2004). *Kwalitatieve analyse: Uitgangspunten en procedures*.
Yin, R. K. (2003). *Case study research: design and methods* (3rd ed. Vol. 5;5.;). Thousand Oaks, Calif: Sage Publications.

6. Bijlages

- Bijlage A. Voorlopig Model
- Bijlage B. Operationalisering Dimensies Raamwerk
- Bijlage C1. Definitief Model voor validatieslag
- Bijlage C2. Definitief Model na validatieslag
- Bijlage D. Case Study Protocol
- Bijlage E. Interview opzet
- Bijlage F. Afgenomen interviews
- Bijlage G. Coderingsmatrix
- Bijlage H. Validatie vragenlijst respondenten
- Bijlage I. Uitkomst validatie respondenten

Bijlage A. Voorlopig Model



Bijlage B. Operationalisering Dimensies Raamwerk

Proces Volwassenheid		De volwassenheid van een organisatie kan bepaald worden door het gebruik van onderstaande tabel. Indien een bewering Grotendeels waar is (minstens 75% waar) wordt het vlak gevuld met de kleur groen; als de bewering Deels waar/Deels niet waar is (tussen 25% en 75% waar) wordt het vlak gevuld met de kleur geel; en als de bewering Grotendeels niet waar is (minder dan 25% waar) dan wordt het vlak gevuld met de kleur rood. Aan de hand van het totaaloverzicht kan het generieke volwassenheidsniveau van de organisatie bepaald worden.						GROEN: Grotendeels waar	GEEL: Deels waar/Deels niet waar	Rood: Grotendeels niet waar		
		Ad-Hoc	Engaged	Structured	Managed	Optimized		Ad-Hoc	Engaged	Structured	Managed	Optimized
Ontwerp	Doel	Het doel van sommige processen is bekend.	Het doel van alle processen is bekend binnen het bedrijf.	Alle processen zijn van begin tot einde ontwerpen om maximale effectiviteit te garanderen.	De processen zijn zo ontwerpen dat zij matchen met elkaar en de aanwezige IT-systemen.	De processen in het bedrijf zijn volledig in lijn met klant en leveranciers processen en bevorderen maximale effectiviteit en efficiency.						
	Documentatie	Er is geen documentatie aanwezig van de processen.	De meeste van de processen zijn helder en zijn gedocumenteerd.	Alle processen zijn beschreven en er is duidelijkheid hoe deze van begin tot einde verlopen.	De documentatie beschrijft de correlatie tussen de verschillende bedrijfsprocessen en de afhankelijkheden zijn duidelijk.	Er is een digitale database met alle bedrijfsprocessen, de koppelingen en er zijn meetbare prestatie indicatoren.						
Gebruikers	Kennis	Sommige spelers in het proces kennen de structuur.	Alle spelers in een proces zijn op de hoogte van de procesflow.	Kennis van de bedrijfsprocessen is wijdverspreid binnen het bedrijf.	Medewerkers zijn bekend met en opgeleid in proces verbeterende technieken.	Medewerkers gaan actief op zoek naar verbetermogelijkheden van processen en er is de ruimte om deze aan te passen.						
Eigenaar	Identiteit	Proces eigenaren zijn niet of nauwelijks gedefinieerd.	Proceseigenaren zijn bekend.	De rol van Proceseigenaar is officieel gecreëerd en deze zijn verantwoordelijk voor verbeteringen.	De proceseigenaar heeft het proces als hoofddoel en heeft de bevoegdheid en middelen om verbeteringen door te voeren.	De proceseigenaar heeft een visie en roadmap voor het bestaande proces en hij/zij is onderdeel van het besluitvormingsproces van het bedrijf.						
ICT infrastructuur	IT-Systemen	Processen worden nauwelijks ondersteund door IT-systemen.	Processen worden ondersteund door specifiek IT-componenten.	Een geïntegreerd IT-systeem ondersteund de processen, welke ook ontworpen is met oog op het proces.	Processen worden volledig ondersteund door IT oplossingen en deze IT-systemen zijn in beperkte mate met elkaar verbonden.	Er is een volledig geïntegreerd systeem, moduleerbaar en volgens standaarden ontwikkelde IT-architectuur.						
Statistieken	Definitie	Er zijn geen statistische indicatoren.	Er is in beperkte mate inzicht op de werken van de processen.	De processen hebben indicatoren die de verschillende vereisten meten.	De processen worden door het hele proces heen gemonitord op de werking.	De processtatistieken worden cross-proces volledig bijgehouden en hier wordt ook op gestuurd.						

Mate van Digitalisatie		De volwassenheid van een organisatie kan bepaald worden door het gebruik van onderstaande tabel. Indien een bewering Grotendeels waar is (minstens 75% waar) wordt het vlak gevuld met de kleur groen; als de bewering Deels waar/Deels niet waar is (tussen 25% en 75% waar) wordt het vlak gevuld met de kleur geel; en als de bewering Grotendeels niet waar is (minder dan 25% waar) dan wordt het vlak gevuld met de kleur rood. Aan de hand van het totaaloverzicht kan het generieke volwassenheidsniveau van de organisatie bepaald worden.										
								GROEN: Grotendeels waar	GEEL: Deels waar/Deels niet waar	Rood: Grotendeels niet waar		
		Ad-Hoc	Engaged	Structured	Managed	Optimized		Ad-Hoc	Engaged	Structured	Managed	Optimized
Middelen	Apparatuur/Hardware	Middelen worden zonder groter plan of visie aangeschaft.	Er is in beperkte mate beleid voor de aanschaf van middelen.	Middelen worden volgens een bepaalde visie en standaard aangeschaft en ingezet met het oog op de specifieke bedrijfsbehoeften.	Alle hardware wordt aangeschaft en ingezet volgens een vooraf opgesteld plan en aan de hand van de geformuleerde architectuur.	Er wordt geen hardware toegestaan die niet voldoet aan de visie en standaarden van het bedrijf.						
	Software	Software wordt ad-hoc gekocht dan wel gedownload.	Software wordt waar mogelijk bedrijfsbreed beoordeelt en vervolgens aangeschaft.	De software ondersteund zo effectief mogelijk de verschillende processen binnen het bedrijf.	De software van de verschillende processen is deels met elkaar verbonden en hier is in sommige mate een vorm van analyse op uit te voeren.	Er is sprake van ERP-systeem achtige software welke door alle processen heen in verbinding staat met elkaar. Hier wordt actief op gemonitord en verbeteringen voor de processen worden door de software mogelijk gemaakt.						
	Automatisering	Er is praktisch geen sprake van automatisering.	Bepaalde processen zijn verrijkt met IT componenten	Bepaalde processen zijn gedigitaliseerd.	Sommige processen zijn geautomatiseerd.	Alle processen zijn volledig geautomatiseerd en deze processen zijn met elkaar verbonden.						
Kennis	Kennis	Er is praktisch geen kennis over de aanwezige IT systemen binnen het bedrijf.	Er is beperkte kennis van de IT systemen aanwezig in het bedrijf.	Er is kennis van de aanwezige systemen en er wordt in beperkte mate ook gedaan aan kennisopbouw.	Er is een actief programma binnen de organisatie om kennis op te bouwen over IT en er zijn voldoende scholingsmogelijkheden voor het personeel.	Het kennis niveau binnen de organisatie zit op een zeer hoog niveau en er wordt onderzoek gedaan naar toekomst mogelijkheden.						
Architectuur	Proces	Er is geen of alleen ad-hoc architectuurproces.	De IT architectuur is beschreven, hier zijn ook duidelijke rollen in aangegeven.	De IT-architectuur is goed uitgewerkt en zowel IT-personeel als het management is hiervan op de hoogte.	De IT-architectuur maakt onderdeel uit van de bedrijfscultuur en wordt actief gemonitord op zijn prestaties.	Er wordt continue gezocht naar optimalisatie van de IT-architectuur en verbeteringen van het proces worden doorgevoerd.						
Management	Documentatie	De gebruikte ICT binnen het bedrijf is niet gedocumenteerd.	Er is een soort van overzicht van de aanwezige hardware en software.	Er is een goed gedocumenteerd overzicht van de aanwezige hardware en software, en dit wordt ook actief bijgehouden en gecontroleerd.	Hardware en software worden actief gemanaged door een beheerorganisatie.	Er is volledig overzicht van de bedrijfsbrede middelen, hier wordt actief beheer op gepleegd.						
	Doelstelling	Er zijn geen doelstelling geformuleerd voor de gebruikte technologie.	Er is in beperkte mate inzicht in de doelstellingen die IT moet ondersteunen.	In grote mate zijn doelstellingen geformuleerd welke door IT behaald moeten worden. Hierbij is er een koppeling gemaakt naar de bedrijfsprocessen die essentieel zijn voor de organisatie.	Er is een duidelijk organisatie doel voor ogen welke ondersteund moet worden door de aanwezige IT middelen. Deze middelen worden proces overstijgend ingezet.	De aanwezige IT middelen en bedrijfsprocessen vormen een intrinsiek geheel en worden in nauwe coördinatie met elkaar constant verbeterd.						

Mate van Cybersecurity		De volwassenheid van een organisatie kan bepaald worden door het gebruik van onderstaande tabel. Indien een bewering Grotendeels waar is (minstens 75% waar) wordt het vlak gevuld met de kleur groen; als de bewering Deels waar/Deels niet waar is (tussen 25% en 75% waar) wordt het vlak gevuld met de kleur geel; en als de bewering Grotendeels niet waar is (minder dan 25% waar) dan wordt het vlak gevuld met de kleur rood. Aan de hand van het totaaloverzicht kan het generieke volwassenheidsniveau van de organisatie bepaald worden.						GROEN: Grotendeels waar	GEEL: Deels waar/Deels niet waar	Rood: Grotendeels niet waar		
		Initial	Basic	Capable	Efficiency	Optimizing		Initial	Basic	Capable	Efficiency	Optimizing
Identificeren	Inzicht in middelen	Er is geen overzicht en/of inzicht in de aanwezige hardware en software.	Er is een soort van overzicht van de aanwezige hardware en software.	Er is een goed gedocumenteerd overzicht van de aanwezige hardware en software, en dit wordt ook actief bijgehouden en gecontroleerd.	Hardware en software worden actief gemanaged door een beheerorganisatie.	Er is volledig overzicht van de bedrijfsvrede middelen, hier wordt actief beheer op gepleegd en kwetsbaarheden zijn bekend en indien mogelijk gemitigeerd.						
	Digitale voetafdruk	Er is geen overzicht van de digitale voetafdruk van het bedrijf.	Er is een globaal overzicht van de digitale voetafdruk van het bedrijf.	Er is een structureel en gedocumenteerd overzicht van alle web en social media platformen waar het bedrijf op actief is.	Er wordt actief gecontroleerd wat er zich afspeelt binnen de digitale voetafdruk van het bedrijf.	Er wordt actief op zoek gegaan naar de digitale mogelijkheden om het bedrijf te benaderen en of deze allemaal juist zijn geconfigureerd.						
Beschermen	Bescherming	Geen of sommige systemen worden voorzien van updates.	Het grootste deel van de systemen wordt regelmatig voorzien van updates. Er is een policy met betrekking tot wachtwoorden.	Het bedrijf beperkt het gebruik van verwijderbare media zoals USB-sticks en SD-kaarten. De firewall is actief. Wachtwoord policies zijn naar de huidige standaard.	Updates van besturingssystemen, applicaties en antivirussoftware wordt structureel uitgevoerd.	Toegang tot systemen en data is beschreven en alleen mogelijk voor geautoriseerde personen.						
	Awareness	Awareness van het personeel komt niet of nauwelijks aan de orde.	Awareness wordt af en toe behandelt.	Medewerkers weten cybercrime te herkennen.	Awareness komt structureel aan de orde en medewerkers weten hoe te handelen bij cybercrime.	Medewerkers worden geschoold in cybersecurity en er is een constante actieve awareness campagne.						
Opsporen	Monitoring	Antivirus is niet of nauwelijks aanwezig.	Antivirussystemen zijn grotendeels aanwezig.	Antivirussystemen zijn verplicht en up to date.	Het bedrijf scant actief op malware en andere dreigingen.	Het bedrijf maakt gebruik van IDS/IPS en monitored zijn systemen continue.						
Reactie	Mitigatie	Er is geen of nauwelijks besef wat er gedaan moet worden bij een mogelijk incident.	Er is een redelijk idee wat er gedaan moet worden bij een mogelijk incident.	Er is beschreven wat er gedaan moet worden bij een mogelijk incident en er zijn mitigerende maatregelen.	Er zijn procedures om een incident te beperken, mitigerende maatregelen zijn in place.	Na een incident wordt er analyse uitgevoerd op de herkomst en oorzaak van het incident. Er wordt lering uit getrokken en actief op zoek gegaan naar nieuwe kwetsbaarheden en de impact daarvan op het bedrijf.						
Herstellen	Herstel	Er worden geen back-ups gemaakt, of alleen sporadisch.	Het bedrijf heeft beleid bepaald ten aanzien van het maken van back-ups.	Het bedrijf maakt regelmatig een back-up van lokale data.	Het bedrijf maakt regelmatig een back-up van alle relevante data in de Cloud en off-site.	De back-up kan worden teruggezet. Het terugzetten van een back-up is getest.						

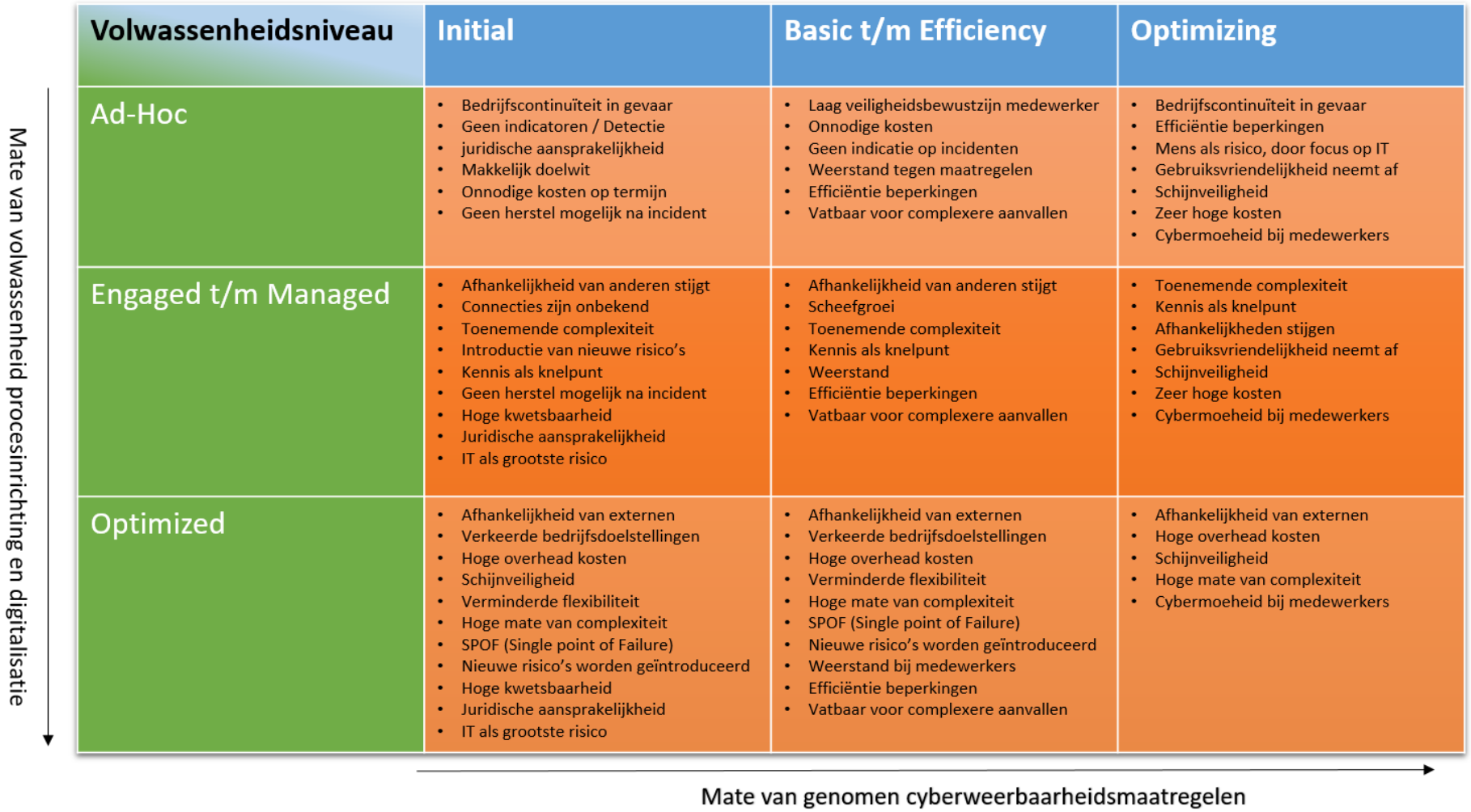
Bijlage C1. Definitief Model voor validatieslag

Mate van genomen cyberweerbaarheidsmaatregelen

Mate van volwassenheid procesinrichting en digitalisatie

Volwassenheidsniveau	Initial	Basic t/m Efficiency	Optimizing
Ad-Hoc	• Bedrijfscontinuïteit • Geen indicatoren / Detectie • Wettelijke aansprakelijkheid • Makkelijk doelwit / kwetsbaar • Onnodige kosten op termijn • Geen herstel	• De medewerker • Onnodige kosten • Geen indicatie op incidenten • Weerstand tegen maatregelen • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Bedrijfscontinuïteit in gevaar • Efficiëntie beperkingen • Mens als risico factor • Gebruiksvriendelijkheid neemt af • Schijnveiligheid • Zeer hoge kosten • Cybermoeheid
Engaged t/m Managed	• Afhankelijkheid van anderen stijgt • Connecties zijn onbekend • Scheefgroei • Toenemende complexiteit • Introductie van nieuwe risico's • Kennis als knelpunt • Geen herstel • Hoge kwetsbaarheid • Juridisch aansprakelijk • IT als grootste risico	• Afhankelijkheid van anderen stijgt • Scheefgroei • Toenemende complexiteit • Kennis als knelpunt • Weerstand • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Toenemende complexiteit • Kennis als knelpunt • Afhankelijkheden stijgen • Gebruiksvriendelijkheid neemt af • Schijnveiligheid • Zeer hoge kosten • Cybermoeheid
Optimized	• Afhankelijkheid van externen • Verkeerde doelstellingen • Hoge overhead kosten • Schijnveiligheid • Verminderde flexibiliteit • Hoge mate van complexiteit • SPOF • Nieuwe risico's worden geïntroduceerd • Hoge kwetsbaarheid • Juridisch aansprakelijk • IT als grootste risico	• Afhankelijkheid van externen • Verkeerde doelstellingen • Hoge overhead kosten • Verminderde flexibiliteit • Hoge mate van complexiteit • SPOF • Nieuwe risico's worden geïntroduceerd • Weerstand • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Afhankelijkheid van externen • Verkeerde doelstellingen • Hoge overhead kosten • Schijnveiligheid • Hoge mate van complexiteit • Cybermoeheid • Hoge mate van complexiteit

Bijlage C2. Definitief Model na validatieslag



Bijlage D. Case Study Protocol (Brereton et al., 2008)

1. Background

Uit onderzoek blijkt dat er weinig wetenschappelijk materiaal is voor het bepalen van cybersecurity binnen het MKB wat betreft risico's voor de bedrijfsvoering. Veel van de beschikbare cybersecurity-criteria zijn opgesteld door cybersecurityinstellingen, maar dienen uitgevoerd te worden door security professionals, EDP-auditors of ander gespecialiseerd personeel. De onderzoeksvraag die we hieruit ontleden is: Hoe ziet een raamwerk eruit waarmee een MKB-ondernemer inzichtelijk krijgt welke risico's hij loopt voor zijn bedrijfsvoering, vanwege onvoldoende genomen cyberweerbaarheidsmaatregelen? Sub vragen die hiervoor eerst beantwoord moeten worden zijn:

1.1. Welke modellen zijn er al bekend ter beoordeling van de 'mate van volwassenheid procesinrichting' en welk model kan als determinant dienen voor het MKB?

1.2. Welke modellen zijn er al bekend ter beoordeling van de 'mate van digitalisering' en welk model kan als determinant dienen voor het MKB?

1.3. Welke modellen zijn er al bekend ter beoordeling van de genomen cybersecuritymaatregelen en welk model kan als determinant dienen voor het MKB?

1.4. Hoe zijn de reeds bestaande modellen te synthetiseren tot een raamwerk?

2. Design

Er is gekozen voor een embedded case design; Verschillende parameters welke op zich zelf zijn geanalyseerd en vervolgens samenkomen in het definitieve model.
Hieruit komt een model naar voren welke de cyberrisico's voor het MKB toont. Waarna de volgende vragen worden beantwoord.

2.1. Hoe is het ontwikkelde model toe te passen op een MKB-organisatie?

2.2. Welke risico's zijn te verbinden aan de verschillende niveaus van het ontwikkelde model?

2.3. Op welke manier is de validiteit van het model te meten?

3. Case Selection

De benodigde informatie kan verkregen worden door specialisten te interviewen(Saunders et al., 2016). De interviews worden afgenomen met verschillende specialisten om de risico's in kaart te brengen. Dit betreft zowel security specialisten met een diepgaande technische kennis als ook security specialisten die meer op management en organisatieniveau werkzaam zijn. De selectie is op basis van de functie, dan wel de certificeringen die een persoon doorlopen heeft. Dit alles met als insteek respondenten te selecteren die zo objectief mogelijk en tevens zo kundig mogelijk een vertaalslag kunnen maken van kwetsbaarheden naar impact. Omdat het hier een relatief homogene onderzoekspopulatie betreft is het doel om vier tot tien specialisten te interviewen en te stoppen op het moment dat er saturatie optreedt in de antwoorden.

4. Case Study Procedures

Tijdens het kwalitatieve onderzoek wordt er gebruik gemaakt van semigestructureerde interviews. Dit zijn zowel diepte interviews als ook expert interviews.

5. Data Collection

De semigestructureerde interviews zullen digitaal worden opgenomen en vervolgens worden uitgewerkt middels het vragenformulier in transcripten. Door het gebruik van transcripten is het mogelijk om door middel van een iteratief proces na elk interview het raamwerk tegen het licht te houden en de vragen in een volgend interview nog gerichter te kunnen formuleren.

6. Analysis

Stap 1. Samennemen/synthetiseren van de interviewantwoorden per dimensie.
Per empirische onderzoeksvraag wordt een samenvatting opgesteld van de gegeven antwoorden en worden deze stuk voor stuk opgenomen in de coderingsmatrix (bijlage G)
Stap 2. Samennemen van de 3 dimensies.
Vervolgens worden op basis van vergelijkingen en codering de deelvragen beantwoord. Hierbij wordt in de coderingsmatrix middels codes gezocht naar overeenkomsten. Deze gedestilleerde overeenkomsten worden vervolgens afgezet tegen de karaktereigenschappen van de verschillende constructen (Bijlage B). Door deze tegen elkaar af te zetten blijven er een aantal restrisico's per niveau over en wordt het ontwikkelde raamwerk gevuld.

7. Validity

Bij de validiteit van een onderzoek is het belangrijk dat de onderzoeksmethode en resultaten correct zijn (Saunders et al., 2016). Een aantal aspecten die de validiteit zouden kunnen benadelen zijn;

- Non-response
- Self-selection

Daarnaast wordt er ook gekeken naar de aspecten Betrouwbaarheid en de ethische aspecten volgens de principes van onderzoek.

8. Study Limitations

- De beperkte tijd die beschikbaar is voor het onderzoek zorgt ervoor dat het aantal te interviewen personen redelijk beperkt moet blijven.
- Het is in dit onderzoek niet mogelijk om het model ook daadwerkelijk te testen bij het MKB, dit zou wel een mooi vervolg onderzoek kunnen opleveren.

9. Reporting

Dit onderzoek maakt onderdeel uit van een onderzoek naar het verhogen van de cyberweerbaarheid van het MKB. Daarnaast wordt er door een mede-onderzoeker gekeken vanuit het oogpunt van de MKB'er op basis van surveys. Voor dit specifieke onderzoek zal er uiteindelijk een rapport worden opgesteld met de onderzoeksresultaten en een model welke gebruikt kan worden door het MKB om de restrisico's op het gebied van cyberdreigingen te visualiseren.

10. Schedule

Geplande tijd voor de verschillende aspecten:

I. Planning: 2 maanden
II. Data collectie: 3 maanden
III. Data analyse: 2 maanden
IV. Rapport uitwerken: 3 maanden

11. Appendices

Veel van de uitwerkingen en de data verzamelingen zullen worden toegevoegd als bijlage.

Bijlage E. Interview Opzet

1. Intro

1.1. Aanleiding tot het interview

Dit interview maakt deel uit van een afstudeeronderzoek aan de faculteit Management, Science & Technology van de Open Universiteit Nederland. In dit onderzoek wordt ingegaan op de risico's van cybercrime en hoe het MKB zich daartegen kan wapenen. Door middel van inzicht in de te beschermen categorieën wordt de cyber weerbaarheid van deze organisaties aan het licht gebracht. Want juist deze groep ondernemingen is steeds vaker slachtoffer van cybercrime (Chabinsky, 2013). In een recent onderzoek onder bedrijven over de hele wereld is gebleken dat veel bedrijven niet intensief genoeg op zoek gaan naar de risico's die het bedrijf in het digitale domein loopt (Castelli, Gabriel, Yates, & Booth, 2018). Dit onderzoek toont aan dat grote multinationals al problemen hebben om grip op cybercrime te krijgen en dat het MKB zich hier al helemaal niet tegen weet te wapenen. Daar komt bij dat cyber security nog altijd wordt gezien als een overhead kostenpost en niet als een intrinsiek onderdeel van de bedrijfsvoering (Ashrafi & Kuilboer, 2001).

Het doel van het interview is om het ontwikkelde model en de categorieën die hiervoor zijn gebruikt te voorzien van de risico's die een MKB-onderneming loopt ten opzichte van zijn bedrijfsprocessen aan de hand van de genomen cyberweerbaarheidsmaatregelen.

1.2. Opzet van het interview

Dit interview betreft een semigestructureerd interview. Dat wil zeggen dat alle geïnterviewden volgens een bepaalde lijst van geselecteerde topics bevraagt zullen worden. Tijdens het interview zal de verdieping op de specifieke topics worden gemaakt aan de hand van de aanwezige expertise. De interviewer zal tijdens het interview de specifieke topics en het ontwikkelde referentiemodel zo nodig toelichten. Bijgevoegd aan dit interview document zijn de verschillende matrixen waarop de volwassenheidsmodellen zijn gebaseerd.

In het interview zal eerst een aantal vragen worden gesteld over de geïnterviewde. Vervolgens wordt ingegaan op de categorieën die zijn gekozen om de risico's te meten en zullen deze aan de hand van de geoperationaliseerde categorieën stuk voor stuk worden behandeld.

De duur van het interview is ongeveer 2 à 3 uur. Het interview kan worden opgenomen en er worden aantekeningen gemaakt. Na afloop zal er door de interviewer een verslag worden gemaakt waarbij de antwoorden behorende bij de verschillende topics zullen worden samengevat. Er wordt gekozen voor een samenvatting ten einde het coderingsproces naderhand te versnellen. Gevoelige en vertrouwelijke informatie zal niet worden vastgelegd. De verslagen met hun bevindingen zullen geanonimiseerd worden toegevoegd aan het onderzoek.

2. Algemene vragen

Dit deel is bedoeld om algemene informatie over de geïnterviewde te verkrijgen.
Per geïnterviewde:

- Wat is uw functie en werkervaring?
- Wat is uw idee van het begrip cybersecurity?
- Hoe veilig denkt u dat MKB'ers zijn op het gebied van cybersecurity?

3. Bedrijfsprocessen

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus van processen en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
- Engaged
- Structured
- Managed
- Optimized

4. Digitalisatie

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus m.b.t. de mate van digitalisatie en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
- Engaged
- Structured
- Managed
- Optimized

5. Cyberweerbaarheidsmaatregelen

Welke Cyber risico's worden er wel of juist niet afgedekt in de verschillende niveaus van cybersecurity gekeken naar het MKB?

- Initial
- Basic
- Capable
- Efficiency
- Optimizing

6. Cyberrisico's voor het MKB

Zijn er buiten de benoemde risico's nog andere risico's die niet aan de orde zijn gekomen tijdens het behandelen van de categorieën?

7. Ontwikkelde raamwerk

Heeft u nog aan- en/of opmerkingen op het ontwikkelde raamwerk?

8. Afsluiting van het interview

8.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, opmerkingen en/of aanbevelingen voor het onderzoek te geven.

- Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?

8.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek. Tevens zal het verslag ter goedkeuring worden toegezonden voor deze verwerkt wordt in het onderzoek.

Bijlage F. Afgenomen Interviews

Te interviewen persoon	Datum gepland	Interview afgenomen	Verslag uitgewerkt
IT-auditor – RE	26-2-2020	26-2-2020	10-3-2020
CEH - Certified Ethical Hacker	27-3-2020	02-4-2020	17-4-2020
CERT - Functionaris	19-4-2020	Niet mogelijk	n.v.t.
CISO - Overheid	27-4-2020	Niet mogelijk	n.v.t.
Hoofd SOC	19-2-2020	19-2-2020	10-3-2020
Security Adviseur en IT-auditor	21-2-2020	21-2-2020	10-3-2020
CISO	02-3-2020	02-3-2020	10-3-2020
Security Analist	Back-up	Niet mogelijk	n.v.t.
CISSP/OSCP	Back-up	Niet mogelijk	n.v.t.
Adviseur Informatiebeveiliging/FG	30-4-2020	25-05-2020	02-06-2020

Interview Nr. 1 – H-SOC

1. Intro

Interview nummer:	1
Plaats interview:	Breda
Datum interview:	19-2-2020
Tijdstip interview:	15:00 – 17:00

2. Algemene vragen

Dit deel is bedoeld om algemene informatie over de geïnterviewde te verkrijgen.
Per geïnterviewde:

- Wat is uw functie en werkervaring?
    - Functie betreft Hoofd-SOC binnen de Overheid, hiervoor cybersecurity adviseur en incident handling. 5 jaar werkervaring. Waarbij de focus niet allen op het technische ligt, maar juist ook op het procesmatige. Dit betekent ook zaken zoals het inrichten van Incident Response.
- Wat is uw idee van het begrip cybersecurity?
    - Alles wat te maken heeft met de verdediging van digitale systemen, dus ook de Human-Machine interface.
- Hoe veilig denkt u dat MKB'ers zijn op het gebied van cybersecurity?
    - 90% van de MKB'ers en kleine ondernemers is niet Cyber secure. Bij deze 90% kan een doorsnee hacker (met als drijfveer financieel gewin) met niet al te complexe aanvallen en binnen niet al te lang tijd zichzelf makkelijk toegang verschaffen tot de systemen van deze ondernemer.

3. *Bedrijfsprocessen*

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus van processen en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Grootste risico zit in het niet kunnen waarborgen van de Business Continuity, omdat er geen structuur is er ook niks om op terug te vallen bij eventuele problemen.
    - Doordat alles ad-hoc gebeurt is er geen focus op efficiency en effectiviteit, dit resulteert vrijwel altijd in het onnodige verlies van capaciteit en bedrijfsmiddelen.
    - Doordat er niets gedocumenteerd is, wordt het ook zeer lastig om dit te evalueren en dus een professionaliteit slag uit te voeren.
- Engaged / Structured / Managed
    - De risico's in deze categorieën liggen allemaal in het verlengde van of in een bepaalde mate ten opzichte van de risico's die benoemd zijn in zowel Ad-Hoc als Optimized.
- Optimized
    - Als alles tot in de kleinste details is vastgelegd kan dit ervoor zorgen dat verandering zeer lastig wordt, alles is zo rigide dat innovatie en flexibiliteit lastig door te voeren zijn.
    - Door in deze mate van procesvolwassenheid te (willen) zitten kan het gevaar bestaan dat het proces een doel op zich wordt en daardoor de focus op het product verdwijnt.

    - Door het tot in de details alles beschrijven en monitoren bestaat de kans op micromanagement, wat dan weer resulteert in het verlies van het doel uit het oog.
    - Door de focus op maximale procesvolwassenheid wordt het doel maximale mogelijkheid tot innovatie in plaats van verbetering. Dit kan zorgen voor te veel afhankelijkheden, denk hierbij aan het plaatsen van het volledige kassasysteem in de Cloud, bij een internetstoring zijn er dan helemaal geen transacties meer mogelijk.

4. Digitalisatie

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus m.b.t. de mate van digitalisatie en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Door het steeds verder uitbreiden van IT zonder een doordacht plan wordt de IT opgestapeld zonder goed naar de comptabiliteit hiervan te kijken, welke met elke toevoeging resulteert in een grotere kans op het instorten van een deel of het hele IT-netwerk.
    - Het gebrek aan automatisering is per definitie een gebrek aan optimalisatie en daardoor een verkwisting van bedrijfsassets.
    - Door in de laagste trede van mate van digitalisatie te blijven hangen, ontstijgt een onderneming het niveau van "huis, tuin & keuken" IT niet en zal daardoor dus ook nooit de kennis voor herstel in huis hebben.
    - Door het zonder plan hebben van IT, is het vrijwel zeker dat er eiland werking optreed. Hiermee wordt bedoeld allerlei op zichzelf staande systemen en applicaties zonder enige vorm van samenwerking.
    - Door het hebben van IT zonder plan liggen onverwachte en onnodige IT-kosten altijd op de loer.
- Engaged
    - Gradatie van de risico's die genoemd zijn in de onder en bovenliggende niveaus.
- Structured
    - In deze fase mist de borging van de specifieke kennis van applicaties en systemen, hierdoor is de kans op verval van deze systemen altijd aanwezig.
    - Door onvoldoende afstemming en integratie wordt het IT-landschap van de organisatie zo complex dat het overzicht verdwijnt.
    - Door het koppelen van applicaties en systemen zonder echt goede integratie wordt de beveiliging steeds moeilijker en verdwijnt natuurlijke segmentatie.
- Managed
    - Gradatie van de risico's die genoemd zijn in de onder en bovenliggende niveaus.
- Optimized
    - Kans op onnodig hoge IT-kosten door een overkill aan IT-middelen.
    - De onderneming kan beperkt worden door de complexiteit van het systeem en de afhankelijkheid van software waar de onderneming zich aan geconformeerd heeft.
    - Innoveren kan een doel op zich worden en niet meer als oplossing voor bestaande problemen.
    - De kans op overmatige focus op randprocessen wordt steeds groter naarmate de mate van digitalisatie stijgt. Niet elke muis hoeft geregistreerd te worden.

5. Cyberweerbaarheidsmaatregelen

Welke Cyber risico's worden er wel of juist niet afgedekt in de verschillende niveaus van cybersecurity gekeken naar het MKB?

- Initial
    - Vulnerability management is zeer lastig als je geen vorm van security hebt.
    - De meest bekende en simpele kwetsbaarheden kunnen makkelijk uitgebuit worden.
    - Malware en Ransomware hebben vrij spel op de systemen zonder kans op ontdekking tot het te laat is.
    - De onderneming is zeer kwetsbaar voor Phising en Social eniginering aanvallen.
    - Herstel is zeer lastig tot vrijwel onmogelijk in dit stadium.
- Basic
    - Gradatie van de risico's die genoemd zijn in de onder en bovenliggende niveaus.
- Capable
    - Bestaande systemen kunnen overbelast raken door detectiesystemen hieraan toe te voegen.
    - Medewerkers kunnen door verkeerde cyber awareness focus paranoïde raken.
    - Misbalans kan ontstaan tussen security en effectiviteit.
- Efficiency
    - Gradatie van de risico's die genoemd zijn in de onder en bovenliggende niveaus.
- Optimizing
    - Door te veel focus op security kan er scheefgroei ontstaan ten opzichte van IT-beheer.
    - Het verhogen van security resulteert vrijwel altijd in het dalen van de usability, dit mag niet overdreven worden.
    - Bij overmatige focus op awareness bestaat de kans dat medewerkers "cybermoe" worden en de aandacht op het onderwerp juist verslapt.
    - Als een organisatie te voorzichtig wordt, bestaat de kans op het gaan controleren van alles wat de effectiviteit van de organisatie weer in het gedrang kan brengen.
    - Optimaliseren van de IDS/IPS kan ervoor zorgen dat er daadwerkelijke alerts worden uitgefilterd.
    - Overmatige kosten en effort door te veel recovery capaciteit.

6. Cyberrisico's voor het MKB

Zijn er buiten de benoemde risico's nog andere risico's die niet aan de orde zijn gekomen tijdens het behandelen van de categorieën?

- Er is een algeheel gemis aan bewustwording bij ondernemers en werknemers binnen het MKB, er heerst nog teveel een sfeer van: "ik ben toch niet interessant" en "er valt bij mij toch niks te halen". Daar komt bij dat er een veelvoud van niet correct geïmplementeerde IT-middelen aanwezig is bij deze ondernemingen welke het attack Surface van de organisatie alleen maar vergroten.

Als we het verder nog hebben over de grootste dreigingen op Cyber vlak voor het MKB dan onderken ik deze drie:

- Malware (ransomware) met grote financiële gevolgen.
- Overtreden van (bijvoorbeeld) de AVG/GDPR door data breaches.
- Misbruik van bedrijf hardware door kwaadwillende partijen.

7. Ontwikkelde raamwerk

Heeft u nog aan- en/of opmerkingen op het ontwikkelde raamwerk?

- Voor de toepasbaarheid en de bruikbaarheid van het raamwerk zou het bij de implementatie ervan helpen om het interactief te maken. Kijk hiervoor ook naar het onderzoek: SOC CCM (Via Google).

8. Afsluiting van het interview

8.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, opmerkingen en/of aanbevelingen voor het onderzoek te geven.

- Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?

Aantal punten:

- Waarom is mate van digitalisatie onderverdeeld in vier categorieën en de andere twee in vijf categorieën?
- Mate van digitalisatie verondersteld dat een onderneming op zijn minst een minimale afhankelijkheid heeft van IT, dat hoeft niet per se zo te zijn.
- Mate van genomen Cyberweerbaarheidsmaatregelen zou voor een IT-zwaar bedrijf dikker aangezet mogen worden.
- Het weten wie je “vijanden” zijn is een belangrijk onderdeel van je risicoanalyse.

8.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek. Tevens zal het verslag ter goedkeuring worden toegezonden voor deze verwerkt wordt in het onderzoek.

Interview Nr. 2 – Security Adviseur en IT-auditor

1. Intro

Interview nummer: 2
Plaats interview: Veldhoven
Datum interview: 21-2-2020
Tijdstip interview: 14:30 – 17:30

2. Algemene vragen

Dit deel is bedoeld om algemene informatie over de geïnterviewde te verkrijgen.
Per geïnterviewde:

- Wat is uw functie en werkervaring?
    - Sinds 10 jaar werkzaam als securityspecialist met betrekking tot het uitvoeren van security scans bij bedrijven en tevens IT-auditor voor zowel wettelijk opgelegde audits als ook audits op verzoek van organisaties zelf.
- Wat is uw idee van het begrip cybersecurity?
    - Er vindt steeds meer een shift plaats naar Cloud services en op die manier dus ook SaaS-diensten. SAAS zorgt op zichzelf voor een heel nieuw scala aan securityproblemen en uitdagingen. Niet op de laatste plaats omdat de verantwoordelijkheid van security zo verwaterd. Ondernemingen denken dat als ze services uitbesteden dat ze ook de risico's uitbesteden.
    - Er is een schifting bezig van klassieke infrastructuur naar SAAS, hierdoor is er steeds meer connectiviteit en bestaat dus het probleem dat ook alle data online staat en mogelijk voor kwaadwillende te benaderen is.
    - Goede cyber security is echt een kwestie van de puntjes op de i zetten, zo niet dat blijf je kwetsbaar.
    - Defense in Depth is het grootste probleem en het feit dat bedrijven zich kunnen verzekeren tegen Cybercrime draagt niet bij aan een goed beschermde organisatie.
    - Cyber security, je doet het goed of je doet het niet.
- Hoe veilig denkt u dat MKB'ers zijn op het gebied van cybersecurity?
    - Absoluut niet veilig, alleen worden de kleinere ondernemingen vooralsnog niet specifiek getarget. Ze worden we meer en meer geraakt door willekeurige aanvallen zoals Ransomware.
    - Daar komt wel bij dat het voor kleine partijen vaak niet te bekostigen is om zich goed te beveiligen. Kleine en middelgrote ondernemers zijn veelal te afhankelijk van hun leveranciers en moeten voldoen aan de eisen en manieren van deze grotere partijen.
    - Daarbij komt dat er ook te veel vertrouwen is in de security van deze grotere serviceproviders en dat het vaak schort aan het hebben van goede SLA's.
    - Door het afnemen van services en het uitbesteden van taken en diensten bestaat er ook steeds minder eigenaarschap van Security en Risk.
    - De hierboven genoemde risico's zijn zaken waar alle ondernemingen tegenwoordig tegenaanlopen, van ZZP'er tot grote onderneming.
    - Diegene waar het wel redelijk op orde is, is als er wetgeving is waar ze aan gehouden worden. Denk hierbij aan PCI, DIGID, etc.

- Uiteindelijk komt het erop neer dat veel ondernemingen aan compliance doen en niet aan security. Het is vaak window dressing en voldoen aan checklists.

3. *Bedrijfsprocessen*

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus van processen en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
  - In dit stadium zijn de individuele werknemers van belang en worden deze dus ook onvervangbaar. Als een persoon wegvalt zijn er geen gegevens over de werkzaamheden en je bent dus als bedrijf afhankelijk van deze personen.
  - In een organisatie waar niets gedocumenteerd wordt, moet steeds opnieuw het wiel uitgevonden worden. Dit lijdt vrijwel altijd tot capaciteitsverlies en verkwisting van resources.
  - Zonder beschreven procedures vindt er ook geen scheiding van verantwoordelijkheden plaats, met alle risico's die daarbij horen van dien.
  - Je loopt als bedrijf grote financiële risico's met betrekking tot de business continuatie.
- Engaged / Structured / Managed
  - Door meer processen te definiëren stijgt ook automatisch de afhankelijkheid van externen, zonder dat deze afhankelijkheden ook altijd helemaal inzichtelijk zijn.
  - Het niet alles in kaart hebben zorgt ook voor problemen bij veranderingen die doorgevoerd worden. Denk bijvoorbeeld aan het aanpassen van IP-adressen, waardoor ineens services van leveranciers niet meer werken. Als deze connecties niet bij iedereen bekend zijn, kan het oplossen van deze problemen zeer lang duren en veel effort kosten.
  - Geen besef van de risico's zolang het werkt, maar door het steeds verder uitbreiden wordt de kans op een catastrofe alleen maar groter.
  - Continuïteit problemen door het steeds meer aan elkaar knopen van processen zonder gedegen plan.
- Optimized
  - In dit stadium ben je vrijwel altijd afhankelijk van andere partijen (leveranciers e.d.) die niet per se op hetzelfde niveau zitten.
  - Er is een volledige afhankelijkheid van IT, bij storing of uitval kun je niets meer.
  - In dit stadium is de flexibiliteit volledig verdwenen en is er dus ook geen aanpassingsvermogen meer aanwezig binnen een bedrijf.
  - Er is in dit stadium een dermate grote afhankelijkheid van services providers, welke door het externe karakter niet te beheersen zijn, dat hier het grootste risico in schuilt.

4. Digitalisatie

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus m.b.t. de mate van digitalisatie en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
  - Je bent al vatbaar voor de basis risico's
  - Je hebt geen idee wat je moet beschermen
  - Er is geen kennis over de services en systemen die je gebruikt in huis.
  - Systemen kunnen uitvallen zonder dat je hiervoor indicatoren hebt gekregen.

    - Er worden juist risico's geïntroduceerd door het niet juist of optimaal inzetten van hard- en software.
- Engaged / Structured / Managed
    - Door beperkte kennis of door het gebruik van de onjuiste middelen worden bedrijfsassets voor de verkeerde taken ingezet.
    - Door meer digitalisatie stijgt ook automatisch de afhankelijkheid van externen, zonder dat deze afhankelijkheden ook altijd helemaal inzichtelijk zijn.
    - Het niet alles in kaart hebben zorgt ook voor problemen bij veranderingen die doorgevoerd worden. Denk bijvoorbeeld aan het aanpassen van IP-adressen, waardoor ineens services van leveranciers niet meer werken. Als deze connecties niet bij iedereen bekend zijn, kan het oplossen van deze problemen zeer lang duren en veel effort kosten.
    - Geen besef van de risico's zolang het werkt, maar door het steeds verder uitbreiden wordt de kans op een catastrofe alleen maar groter.
    - Continuïteit problemen door het steeds meer aan elkaar knopen van soft- en hardware zonder gedegen plan.
- Optimized
    - Overmatige afhankelijkheid van externen
    - Door alles meteen op te volgen (bijvoorbeeld patchmanagement) bestaat er de kans op het negatief beïnvloeden van je business continuïteit, door het niet testen van de uitwerking van updates op je in gebruik zijnde software.
    - De organisatie is volledig afhankelijk van de IT en kan niet doorgaan bij storing of uitval.
    - Door volledige automatisering en integratie is de flexibiliteit en het aanpassingsvermogen zeer beperkt.
    - Er is een groot verschil in de mate van volwassenheid en omgang tussen je fysieke en je digitale leveranciers. Dit vraagt voor elke leverancier een andere aanpak en zorgt dus voor meer complexiteit.

5. Cyberweerbaarheidsmaatregelen

Welke Cyber risico's worden er wel of juist niet afgedekt in de verschillende niveaus van cybersecurity gekeken naar het MKB?

- Initial
    - In dit stadium is een bedrijf zelfs kwetsbaar voor geautomatiseerde aanvallen.
    - De meest bekende en standaard kwetsbaarheden zijn aanwezig binnen het bedrijf.
    - Er is geen segmentatie en daardoor ook geen barrière om een eventuele aanvaller tegen te houden als deze eenmaal binnen is. Dit zorgt er ook voor dat virussen vrije baan hebben als zij eenmaal binnen het netwerk zijn.
    - Er is geen enkele mogelijkheid op herstel als er iets fout gaat.
    - Na verloop van tijd zullen systemen ophouden met functioneren door geen of slecht beheer.
    - Door het niet hebben van inzicht in de aanwezige systemen is er ook geen inzicht in welke kwetsbaarheden de organisatie heeft.
    - Door het steeds meer gebruiken van virtualisatie wordt er steeds minder aandacht besteed aan het fatsoenlijk beheren en inzetten van hardware. Dat wordt nog meer versterkt doordat VM's het makkelijker maken om uit te breiden zonder, in eerste instantie, goed te moeten kijken naar de hardware vereisten.

- Basic / Capable / Efficiency
    - Leveranciers introduceren risico's door het gebruik van andere en/of verouderde software zonder dat hier controle over uitgevoerd kan worden.
    - Sommige systemen werken minder optimaal of niet door de toevoeging van securitymaatregelen.
    - Er bestaat vaak geen mandaat voor de uitvoering van security, dit zorgt ervoor dat goede initiatieven vaak stranden.
    - Er is vaak een gemis aan draagvlak bij de directie voor de uitvoering van belangrijke security aspecten, denk hierbij aan de haven van Rotterdam en het draaien van updates.
    - Schijnveiligheid door het niet volledig zijn in de implementatie van securitymaatregelen.
- Optimizing
    - Het hebben van een 100% overzicht is een utopie en dus kan dit een vals gevoel van veiligheid geven.
    - Cybersecuritymaatregelen zullen altijd omzeild worden in het kader van innovatie.
    - Door hoge mate van security kan de flexibiliteit van de organisatie weggenomen worden.
    - Dit stadium is een mooi streven, maar voor vrijwel elke organisatie niet haalbaar. Tevens ook vanwege het feit dat de schaalbaarheid van IT, niet betaalbaar is op het gebied van security (bijvoorbeeld 50 per maand per werknemer voor Cloud security, bij een organisatie van 10.000 medewerkers).

6. Cyberrisico's voor het MKB

Zijn er buiten de benoemde risico's nog andere risico's die niet aan de orde zijn gekomen tijdens het behandelen van de categorieën?

- De tendens is dat er bij ondernemingen een steeds grotere afhankelijkheid van Cloud en SaaS-diensten komt. Dit zorgt voor een valse mate van vertrouwen, eigenaarschap van risico's wordt steeds minder duidelijk.

- Het steeds grotere aanbod van Cyber Securityverzekeringen zonder fatsoenlijke eisen en standaarden waar deze bedrijven aan moeten voldoen. Dit zorgt voor luiheid en een vals gevoel van veiligheid bij bedrijven.

7. Ontwikkelde raamwerk

Heeft u nog aan- en/of opmerkingen op het ontwikkelde raamwerk?

- Zorg voor een overzichtelijk en niet te complex geheel zodat de MKB'er hier gebruik van kan maken.

- Voor meer diepgang en specifieke risico's is een onderverdeling van MKB-sectoren aan te raden in de toekomst.

8. Afsluiting van het interview

8.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, opmerkingen en/of aanbevelingen voor het onderzoek te geven.

- Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?

8.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek. Tevens zal het verslag ter goedkeuring worden toegezonden voor deze verwerkt wordt in het onderzoek.

Interview Nr. 3 – RE / EDP-Auditor

1. Intro

Interview nummer: 3
Plaats interview: Den Haag
Datum interview: 26-2-2020
Tijdstip interview: 13:00 – 15:30

2. Algemene vragen

Dit deel is bedoeld om algemene informatie over de geïnterviewde te verkrijgen.
Per geïnterviewde:

- Wat is uw functie en werkervaring?
    - RE / EDP-auditor voor de overheid. Werkzaam sinds 5 jaar als auditor, sinds dit jaar Volledig RE opgeleid.
- Wat is uw idee van het begrip cybersecurity?
    - Het is een zeer breed begrip en omvat alle risico's en maatregelen die voor kunnen komen met betrekking tot informatiesystemen. Vooral ook op het moment dat deze enigerwijs een koppeling hebben met internet.
- Hoe veilig denkt u dat MKB'ers zijn op het gebied van cybersecurity?
    - Het MKB is een breed spectrum van bedrijven en deze vraag is dus afhankelijk van de grootte van de organisatie. Grotere MKB zijn zich meer bewust van de risico's dan kleinere bedrijven, dit omdat de grotere bedrijven ook meer aandacht trekken bij digitale criminelen. Er valt bij deze organisaties over het algemeen meer te halen en daar zijn deze bedrijven zich ook meer bewust van. Doordat dit gevoel niet/minder leeft bij kleinere ondernemingen zijn zij kwetsbaarder voor aanvallen.

3. *Bedrijfsprocessen*

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus van processen en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Als er iets misgaat ben je als organisatie meer aansprakelijk omdat je er niks tegen gedaan hebt.
    - De kans dat er iets flink mis gaat is misschien kleiner, maar als er iets mis gaat wordt je hierdoor volledig verrast.
    - Als er iets misgaat is het zeer lastig tot vrijwel onmogelijk om te herstellen omdat er geen basis is om naar terug te herstellen.
    - Processen die niet beschreven/gedocumenteerd zijn, bestaan niet!
    - Alle belangrijke zaken zitten alleen in het hoofd van de medewerkers en deze worden daardoor onvervangbare assets.
    - Hoge mate van in efficiency doordat er niet doordacht naar de processen gekeken wordt.
- Engaged / Structured / Managed
    - Er zal een bepaalde gradatie van de eerdergenoemde risico's zijn, maar waarschijnlijk in mindere mate.
    - De grootste risico's die in deze volwassenheid stappen aanwezig zijn, zijn ondernemingsrisico's en minder cyber risico's.

- Optimized
    - Hoogste vorm van volwassenheid heeft ook te maken met een goed risicomanagement, de restrisico's zouden in dit stadium dus zeer beperkt moeten zijn.

4. Digitalisatie

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus m.b.t. de mate van digitalisatie en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Hoge mate van Shadow-IT aanwezig in de organisatie en daardoor een hoge mate van afhankelijkheid van de medewerkers die dit gebouwd hebben.
    - Verspilling van bedrijfsassets door de afwezigheid van een gedegen kosten-baten analyse bij de aanschaf en inzet van middelen.
    - Geen changemanagement zorgt voor chaos in rechten en beheer.
    - Geen inzicht in wat voor impact de uitval of storing op hard- en software heeft voor het bedrijf.
    - Als je de basis IT-zaken niet op orde hebt ben je zelfs vatbaar voor scriptkiddies en de risico's die onbekwame medewerkers introduceren.
    - Als alles wordt toegestaan op het netwerk is de kans op virus besmettingen zeer groot.
    - Doordat er geen gedegen architectuur aanwezig is, wordt schaalbaarheid van de organisatie zeer lastig en prijzig.
- Engaged / Structured / Managed
    - Geleidelijke schaal van risico's tussen Ad-hoc en Optimized.
- Optimized
    - Introductie van single-point-of-failures voor de organisatie.
    - Overmatig gebruik van VM's waardoor er minder aandacht aan hardware beheer besteed wordt.
    - Software Defined Netwerken zorgen voor grote mate van software afhankelijkheid.
    - Security gaat vaak ten koste van de efficiency.
    - Efficiency zorgt vaak voor het uitbannen van redundantie en dus gemis aan recovery capaciteit.

5. Cyberweerbaarheidsmaatregelen

Welke Cyber risico's worden er wel of juist niet afgedekt in de verschillende niveaus van cybersecurity gekeken naar het MKB?

- Initial
    - Vatbaar voor alle soorten aanvallen, van geautomatiseerd tot en met specifiek getarget.
    - Grote kans op het overtreden van wet- en regelgeving.
    - Continuïteit van het bedrijf staat constant op het spel.
- Basic / Capable / Efficiency
    - In meer of mindere mate aanwezigheid van genoemde risico's bij uitersten van de schaal.
    - Grotere dreiging vanuit de "Interne dader".
- Optimizing
    - De kosten zijn hoger dan de kosten die het eventueel kan besparen.
    - Complexiteit van de geïmplanteerde maatregelen en controls.

- Oog voor het personeel kan verdwijnen door de focus op de techniek.
- Grotere kans op weerstand van het personeel door het beperken van de werkbaarheid.
- Vendor Lock-in: je maakt je als onderneming zo afhankelijk van een enkele partij dat omschakelen of veranderen niet meer mogelijk is of zeer kostbaar wordt.

6. Cyberrisico's voor het MKB

Zijn er buiten de benoemde risico's nog andere risico's die niet aan de orde zijn gekomen tijdens het behandelen van de categorieën?

- Geen overige, dan wel niet eerder benoemde risico's.

7. Ontwikkelde raamwerk

Heeft u nog aan- en/of opmerkingen op het ontwikkelde raamwerk?

- Er is een grote kans dat een MKB'er in meerdere hokjes te plaatsen is.

- Het raamwerk kan een goede manier zijn om inzicht te creëren, het hoeft niet per se structuur te verschaffen.

- Het zal een uitdaging blijven om tussen een zelf-asses checklist te zitten en op het niveau van bijvoorbeeld een NIST framework.

8. Afsluiting van het interview

8.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, opmerkingen en/of aanbevelingen voor het onderzoek te geven.

- Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?
    - Kijk ook eens naar de risico sheets die ontwikkeld zijn door het VNG.

8.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek. Tevens zal het verslag ter goedkeuring worden toegezonden voor deze verwerkt wordt in het onderzoek.

Interview Nr. 4 - CISO

1. Intro

Interview nummer: 4
Plaats interview: Den Haag
Datum interview: 02-03-2020
Tijdstip interview: 12:00 – 14:00

2. Algemene vragen

Dit deel is bedoeld om algemene informatie over de geïnterviewde te verkrijgen.
Per geïnterviewde:

- Wat is uw functie en werkervaring?
    - Als CISO verantwoordelijk voor het informatiebeveiligingsbeleid binnen het bedrijf. Daarbij ligt de focus voornamelijk op het technische gedeelte. Sinds 6 jaar werkzaam binnen cyber (security).
    - Daarnaast ligt de hoofdtaak naar klanten toe op het uitvoeren en implementeren van Network Security Monitoring. Hierbij is vaak de EPD-koppeling tussen techniek en business het grote vraagstuk.
    - In het verleden bezig geweest als incident response handler/coördinator.
- Wat is uw idee van het begrip cybersecurity?
    - Het zo goed mogelijk beveiligen van al je digitale reilen en zeilen.
- Hoe veilig denkt u dat MKB'ers zijn op het gebied van cybersecurity?
    - Vanuit veelvuldig onderzoek is te bevestigen dat dit over het algemeen bij het MKB zeer slecht geregeld is. De ervaring leert dat pas als er echt iets goed fout gegaan is bij een organisatie er op aandacht besteed wordt aan cyber security. Buiten dat wordt "handig" nog steeds boven "veilig" verkozen.
    - Ook als IT uitbesteed wordt naar een andere partij blijkt vaak dat deze service verleners hun security niet voldoende op orde hebben.
    - Dit alles komt doordat voor veel ondernemingen security niets zichtbaar oplevert.
    - Doordat er nog steeds een taboe heerst op het melden van incidenten krijgt het onderwerp security bij veel bedrijven ook niet de aandacht die het zou moeten krijgen. Onbekend maakt onbemind en door het taboe blijft het onbekend hoe groot het risico is.

3. Bedrijfsprocessen

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus van processen en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Als het fout gaat, gaat het ook meteen goed fout.
    - Omdat er geen documentatie is, is er ook geen startpunt om bij eventuele storingen of crashes naar terug te herstellen.
    - De omvang en impact van een incident zijn niet te bepalen door de afwezigheid van inzicht in de organisatie.
    - Iedereen doet maar wat en daardoor is er geen efficiency en effectiviteit binnen het bedrijf.

    - Daar komt bij dat verantwoordelijkheden niet belegd zijn, dus niemand voelt zich verantwoordelijk voor de aanwezige risico's.
    - Er zijn veel en voornamelijk "Unknown-Unknowns"
- Engaged / Structured / Managed
    - In de tussenliggende fases worden er vaak steeds meer zaken gekoppeld, door het niet of maar beperkt inzicht hebben in de hele bedrijfsvoering brengt het koppelen onmiddellijk risico's met zich mee voor de gekoppelde systemen en processen.
    - Geleidelijke schaal van risico's zoals deze in de beide uiterste treden zijn benoemd.
- Optimized
    - Doordat er een dermate interactie met leveranciers is wordt de procesverwevenheid groter dan inzichtelijk is voor de organisatie.
    - De leveranciers inzichtelijkheid kan voor een blindelings en vals gevoel van vertrouwen zorgen.

4. Digitalisatie

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus m.b.t. de mate van digitalisatie en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - De ad-hoc fase slaat vaak op de mens, in deze fase is IT vaak uitbesteed.
    - Het gebruik van IT is in deze fase puur gericht op usabillity en niet op security of sustainability.
    - Een organisatie is in deze fase zelfs kwetsbaar voor de meest simpele en geautomatiseerde aanvallen.
    - De digitale voetafdruk van het bedrijf mag in deze fase dan wel zeer klein zijn, daar waar die aanwezig is, is deze meteen zeer kwetsbaar.
- Engaged / Structured / Managed
    - In de tussenfases wordt de complexiteit steeds groter zonder het daarbij behorende totale overzicht.
    - Automatisering is het meest simpele om te verhogen en dat gaat dus vaak het snelste, maar de stappen die hierbij horen zoals het verbeteren van de documentatie en visie blijven vaak achter omdat deze complexer zijn. De groei in fases is dus vaak niet evenredig wat weer risico's met zich meebrengt.
- Optimized
    - Door volledige verbondenheid is er geen segmentatie en dus ook geen belemmering voor een eventuele aanval om het hele netwerk te bereiken.
    - In deze fase heeft een organisatie vaak een zeer grote digitale voetafdruk en dus per definitie een groot aantal aanval vectoren.
    - De complexiteit is in deze fase zeer groot en maakt het dus lastig en kostbaar dit goed te beheren.

5. Cyberweerbaarheidsmaatregelen

Welke Cyber risico's worden er wel of juist niet afgedekt in de verschillende niveaus van cybersecurity gekeken naar het MKB?

- Initial
    - Geen awareness, betekend geen waakzame medewerkers die iets vroegtijdig kunnen identificeren en/of tegenhouden.
    - Vatbaar voor alle soorten aanvallen.
    - Als er iets misgaat, is de kans ook groot dat het meteen goed fout gaat.

    - In deze fase zitten de grootste risico's in de techniek.
    - Je komt er vaak niet eens achter dat er iets mis is, tot dat het echt te laat is.
    - Herstel is vaak niet mogelijk of zeer lastig en kostbaar.
- Basic / Capable / Efficiency
    - Als het mis gaat zal de impact nog steeds vrij groot zijn, halve herstelmaatregelen zijn meestal niet voldoende.
    - Herstel is lastig.
    - Nog steeds vatbaar voor wat meer complexe aanvallen.
- Optimizing
    - Mens wordt de grootste kritieke factor.
    - Kans bestaat dat het zo dicht zit, dat er een onwerkbare situatie wordt gecreëerd.
    - Zeer prijzig.

6. Cyberrisico's voor het MKB

Zijn er buiten de benoemde risico's nog andere risico's die niet aan de orde zijn gekomen tijdens het behandelen van de categorieën?

- Meeste risico's zijn wel benoemd in de voorgaande vragen.

- Als je aan de uiterste kanten zitten van de volwassenheidsschalen dan loop je voornamelijk business risico's, cyber risico's zitten meer in de tussenliggende niveaus.

7. Ontwikkelde raamwerk

Heeft u nog aan- en/of opmerkingen op het ontwikkelde raamwerk?

- De vraag blijft of het aantal van vijf niveaus juist is om te benoemen. Eigenlijk komt het in alle volwassenheidsschalen erop neer dat je: aan het begin staat, aan het einde bent of dat je er tussenin zit. Dit zorgt ervoor dat de vraag blijft staan of het benoemen van niveaus noodzakelijk is.

- Het niet hebben van een sub verdeling in MKB-sectoren maakt het lastig nog specifiekere risico's te definiëren.

8. Afsluiting van het interview

8.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, opmerkingen en/of aanbevelingen voor het onderzoek te geven.

- Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?
    - Eventueel kan er nog een verificatieslag plaatsvinden met de klantcontactmanager om te bepalen of de gevonden risico's ook aansluiten bij het beeld dat er leeft bij de MKB-organisaties.

8.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek. Tevens zal het verslag ter goedkeuring worden toegezonden voor deze verwerkt wordt in het onderzoek.

Interview Nr. 5 - CEH

1. Intro

Interview nummer: 5
Plaats interview: Helmond
Datum interview: 02-04-2020
Tijdstip interview: 09:00 – 12:00

2. Algemene vragen

Dit deel is bedoeld om algemene informatie over de geïnterviewde te verkrijgen.
Per geïnterviewde:

- Wat is uw functie en werkervaring?
    - Sinds 4 jaar werkzaam als Cyber Security Adviseur binnen de Audit & Control afdeling van een overheidsorganisatie.
    - Hoofdtaak ligt binnen de huidige functie in het uitvoeren van Audits en controle op Cyber security in het aankoop proces.
- Wat is uw idee van het begrip cybersecurity?
    - Combinatie van beleid, maatregelen en cultuur die ervoor zorgen dat “optimale” controle wordt gewaarborgd.
    - Cybersecurity is een middel en geen doel, het zorgt ervoor dat handelingsvrijheid blijft bestaan.
- Hoe veilig denkt u dat MKB’ers zijn op het gebied van cybersecurity?
    - We zitten niet meer in de volledige beginfase, maar we zitten ook zeker nog niet op een professioneel niveau.
    - Awareness is wel ontstaan, maar het gewenste en daarbij behorende gedrag wordt nog niet vertoond.
    - Zie bijvoorbeeld nu met de Corona crisis, we zijn al driemaal gewaarschuwd (SARS, EBOLA, Vogelgriep) mar nu het ons echt raakt gaan we pas handelen. Dit zou je kunnen vergelijken met een wereldwijde Ransomware uitbraak, waarvoor we ook al gewaarschuwd zouden moeten zijn met PetYa en dergelijke.
    - Leeftijd speelt hier zeker een rol, maar de ouderen zijn daar en tegen weer wat makkelijker om door te werken als systemen uitvallen omdat zij gewend zijn op deze manier te werken.

3. Bedrijfsprocessen

Welke Cyber risico’s gekeken naar de vijf volwassenheidsniveaus van processen en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Reactief, je wordt altijd verast.
    - Bij een incident is je hersteltijd zeer lang, vooropgesteld dat deze überhaupt mogelijk is.
    - Waar je voor je gevoel bespaart aan de voorkant, ben je bij een incident vele malen duurder uit.
    - Wettelijk ben je aantoonbaar nalatig geweest.
    - De autoriteit persoonsgegevens zal in deze fase zeker zaken vinden die zij beboeten.
    - Onvolwassenheid van de gehele organisatie.
- Engaged / Structured / Managed

    - Hoe kleiner een bedrijf des te kleiner de kans dat ze geraakt worden, maar als ze geraakt worden is de impact des te groter. Hoe groter een bedrijf is, zal dit vaak andersom werken.
- Optimized
    - You get what you measure.
    - Het middel wordt een doel op zich.
    - Pervers effect → een effect wat je onbewust creëert (De PKI wordt een bedrijfsdoel op zichzelf).
    - Je veranderproces wordt langzamer vanwege alle stappen die beschreven zijn en dus doorlopen moeten worden. Ook omdat alles met elkaar verbonden is en wijzigingen dus niet zomaar doorgevoerd kunnen worden.
    - Deze fase kost je evenredig meer geld omdat je meer overhead hebt.

4. Digitalisatie

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus m.b.t. de mate van digitalisatie en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Je weet niet wat je "echt" binnenhaalt, denk hierbij aan het downloaden van software via Piratebay.
    - Kans om geraakt te worden is veel groter.
    - Omdat je niet de juiste kennis bezit, kies je niet per definitie wat je nodig hebt als organisatie.
- Engaged / Structured / Managed
    - Sub-optimalisatie door beperkt beleid. Ad-hoc geeft hier minder kans op.
    - Je regelt wel iets, maar het is niet afgestemd en in lijn met het grotere doel.
    - Je introduceert meer risico's door modulair te verbeteren i.p.v. integraal. Denk hierbij bijvoorbeeld aan het koppelen van systemen zonder te denken aan aanvullende beveiliging.
    - Door gebrek aan documentatie wordt je harder geraakt door personeelswisselingen, de kennis zit in de mens i.p.v. de organisatie.
- Optimized
    - Je creëert in deze fase een hoge mate van afhankelijkheid van leveranciers → kans op Vendor Lock-in.
    - Keuzes kunnen worden beïnvloed door overstijgende (politieke) belangen.
    - Wijzigingen vragen significant meer handelingen om door te voeren.
    - Hoe meer je weet, des te meer je hebt te doen (Geen Excuus om het niet te doen).

5. Cyberweerbaarheidsmaatregelen

Welke Cyber risico's worden er wel of juist niet afgedekt in de verschillende niveaus van cybersecurity gekeken naar het MKB?

- Initial
    - Je bent vatbaar voor het hele palet van aanvallen en incidenten.
    - Alles binnen je bedrijf kan geraakt of beïnvloed worden.
    - Elk incident kan per definitie catastrofaal zijn.
    - Hard- en software zijn je grootste risico.
- Basic / Capable / Efficiency
    - Gradatie van risico's genoemd bij Initial en Optimizing.
    - Sub-optimalisatie door gedeeltelijke beveiliging.

    - Hoe volwassener de security van hard en software des te groter wordt het risico op social enginering.
    - Cultuur binnen een organisatie kan voor weerstand zorgen.
    - Gedeeltelijke security nodigt uit om “creatief” te boekhouden en alternatieve processen te bewandelen.
- Optimizing
    - Mens wordt de grootste kritieke factor.
    - Hoge kosten.
    - Hoge mate van inspanning om op dit niveau te blijven.
    - Kans op een delta tussen wat je investeert en wat je eruit haalt.
    - Mismatch tussen opvatting van het management en de personeelscultuur.
    - False sense of security, door te denken dat je alles kunt voorkomen of afdekken.

6. Cyberrisico’s voor het MKB

Zijn er buiten de benoemde risico’s nog andere risico’s die niet aan de orde zijn gekomen tijdens het behandelen van de categorieën?

- 90% is wel afgedekt in de bovenstaande antwoorden, de overige 10% zit in de soft-controls van een organisatie. Aanspreken op gedrag is in de NL-cultuur heel wisselvallig en zeer afhankelijk van de persoon.

- Als je aan de uiterste kanten zitten van de volwassenheidsschalen dan loop je voornamelijk business risico’s, cyber risico’s zitten meer in de tussenliggende niveaus.

7. Ontwikkelde raamwerk

Heeft u nog aan- en/of opmerkingen op het ontwikkelde raamwerk?

- Het raamwerk is een prima basis, maar afhankelijk van de specifieke sector zal er zeker nog een verdiepingsslag of specialisatie gedaan moeten worden.

- Een raamwerk kan ondersteunen maar is niet zaligmakend, universeel toepasbaar maakt het een goed startpunt om van daaruit verder te verdiepen.

8. Afsluiting van het interview

8.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, opmerkingen en/of aanbevelingen voor het onderzoek te geven.

- Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?
    - Geen verdere opmerkingen.

8.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek. Tevens zal het verslag ter goedkeuring worden toegezonden voor deze verwerkt wordt in het onderzoek.

Interview Nr. 6 – InfoSec en Privacy

1. Intro

Interview nummer: 6
Plaats interview: Eindhoven
Datum interview: 25-05-2020
Tijdstip interview: 10:00 – 13:00

2. Algemene vragen

Dit deel is bedoeld om algemene informatie over de geïnterviewde te verkrijgen.
Per geïnterviewde:

- Wat is uw functie en werkervaring?
    - Sinds 2 jaar werkzaam als Adviseur Information Security en Privacy.
    - Voornamelijk in de sector Zorg & Care, met af en toe een andere non-profit organisatie.
    - In de jaren ervoor gestart als Informatiemanager en daarna gespecialiseerd op information security, waarna de logische vervolgstap kwam om AVG hierbij te betrekken.
- Wat is uw idee van het begrip cybersecurity?
    - Cyber security is meer de harde kant van de beveiliging gericht op techniek. Daarnaast is information security gericht op de “zachte” management kant, meer gericht op compliance. Daar komt als derde bol nog de privacy kant bij welke voornamelijk een juridisch karakter heeft. Deze drie bollen staan niet los van elkaar, maar overlappen elkaar op de grensgebieden en de combinatie van deze drie zorgt voor een digitaal veilige onderneming.
- Hoe veilig denkt u dat MKB’ers zijn op het gebied van cybersecurity?
    - Niet veilig, op een schaal van 1 tot 10, ongeveer op een 3. Dit is geen afweging op basis van risico’s, maar op een schaalverdeling van niets tot zwaarbeveiligd.
    - Als het misgaat, gaat het ook meteen goed mis bij een MKB’er. Maar het is voor deze sector wel lastig om een risico-kosten afweging te maken.

3. Bedrijfsprocessen

Welke Cyber risico’s gekeken naar de vijf volwassenheidsniveaus van processen en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
    - Geen idee waarom er wat gedaan wordt, er wordt gedaan wat men goed acht.
    - Geen uniformiteit, ook niet richting de klanten.
    - Mens is de onvervangbare asset.
    - Grote kans op de aanwezigheid van Singel Points Of Failure.
    - Je weet niet wat je doet.
- Engaged / Structured / Managed
    - Geen visie brengt een gevaar van scheefgroei met zich mee voor de organisatie.
    - Je moet wel weten wat er nodig is voor je organisatie, zonder door te slaan.
- Optimized
    - Te veel bureaucratie en dus te veel overhead.
    - Deze fase bereiken draagt niet meer bij aan organisatie doelstellingen, het wordt een doel op zich.

- Gebrek aan flexibiliteit.
- Dit is werkbaar voor grote organisaties, voor een MKB'er zit er geen optimalisatieslag in het behalen van dit niveau.
- Inwerken van nieuwe medewerkers duurt op deze manier zeer lang.
- Gaat ten koste van de productiviteit.
- Doel op zich in plaats van een middel.

4. Digitalisatie

Welke Cyber risico's gekeken naar de vijf volwassenheidsniveaus m.b.t. de mate van digitalisatie en de bijbehorende categorieën zijn er te beschrijven voor het MKB?

- Ad-Hoc
  - Schokkend om te zien dat dit het meest voorkomende niveau is voor kleine organisaties.
  - Onsamenhangende brei van hard- en software.
  - Hoe kleiner, des te minder last heb je hiervan, je organisatie is minder complex, dus ook overzichtelijker.
  - Hoe groter, des te groter is het probleem als je op dit niveau zit.
  - Grote kans op onnodige uitgaven, dubbelingen zullen veel aanwezig zijn.
  - Gratis varianten van software brengt een variëteit aan risico's met zich mee.
  - "Chaos kost geld"
- Engaged / Structured / Managed
  - Scheefgroei binnen de maturity stappen, omdat de onderliggende categorieën niet evenredig makkelijk zijn om in te groeien.
  - Kennis op het juiste niveau is een specialisme op zich, wat je dus ook in huis moet hebben.
  - Hoe meer digitalisatie je hebt, des te verder ga je achterlopen op kennisniveau.
  - Ook hier bestaat een grote kans op verscheidene Single Points Of Failure.
- Optimized
  - Het wordt een doel op zich, in plaats van dat je de bedrijfsvoering probeert te verbeteren.
  - Je ontwikkelt een zeer complexe organisatie.
  - Als kleine ondernemer relatief makkelijk om te bereiken, des te groter des te lastiger te bereiken.
  - Zeer prijzig om dit niveau te bereiken, er bestaat een grote kans dat de balans tussen kosten vs. de output kwijtraakt.
  - Grote afhankelijkheid van je digitale middelen.

5. Cyberweerbaarheidsmaatregelen

Welke Cyber risico's worden er wel of juist niet afgedekt in de verschillende niveaus van cybersecurity gekeken naar het MKB?

- Initial
  - Veel voorkomende fase bij veel ondernemingen.
  - Hoe kleiner een organisatie des te groter de kans dat ze op dit niveau zitten.
  - Hoe groter een organisatie des te groter de kans dat er een aantal zaken "per ongeluk" geregeld zijn (bijv. door Cloud services). Dit betekend niet dat ze hier ook inzicht in hebben.
  - Geen kennis over waar je risico's liggen als organisatie.

    - Bedrijf continuïteit komt al snel in gevaar als je in deze fase zit. (Vooral op het aspect beschikbaarheid)
    - Kans op imagoschade is op dit niveau zeer groot (kijk naar het voorbeeld van Zoom).
    - Je bent in deze fase ook echt nalatig en dus juridisch aansprakelijk.
- Basic / Capable / Efficiency
    - De risico's bij een laag maturity niveau zijn duidelijk, hoger niveau is lastig.
    - Wat is de juiste afweging tussen risicoacceptatie en beveiliging, dat is voor een kleine MKB'er lastig te bepalen.
    - Verkeerd inschatten van je risico's.
    - Kans dat je de verkeerde dingen doet.
    - Kans op hoge kosten zonder een evenredig effect bij het verkeerd inzetten van je middelen.
- Optimizing
    - Je streeft als snel het doel voorbij, doordat het een doel op zich wordt.
    - Kans op het creëren van een angstcultuur.
    - Moeilijk om dit niveau goed te managen.
    - Vaak te mooi om waar te zijn.
    - Je moet je afvragen of je hier als MKB'er naartoe moet; als bank wel, als schilder niet.
    - Kosten staan op dit niveau vaak niet in verhouding tot de baten.
    - Een goede risicoafweging is belangrijker dan een zo hoog mogelijke beveiliging.
    - Kans op het creëren van schijnheiligheid.

6. Cyberrisico's voor het MKB

Zijn er buiten de benoemde risico's nog andere risico's die niet aan de orde zijn gekomen tijdens het behandelen van de categorieën?

- Als de niveaus van de verschillende volwassenheidsmaatstaven niet gelijklopen, loop je per definitie risico. De niveaus moeten in balans zijn, op zichzelf zeggen ze niet zo veel, maar in verbinding met elkaar wel.

- Een risico is niet voor niets een risico, ze zijn er altijd en als je er maar van op de hoogte bent kun je ze ook accepteren (Risk appetite).

- Als je iets niet weet kun je er ook niet naar handelen, je moet dus wel meten.

7. Ontwikkelde raamwerk

Heeft u nog aan- en/of opmerkingen op het ontwikkelde raamwerk?

- Het is vaak niet zo zwart-wit als een model schetst.

- Veelal is het een glijdende schaal en zijn de stappen wat meer fluïde.

- De samenhang tussen de verschillende categorieën zal interessante resultaten opleveren

8. Afsluiting van het interview

8.1. Slotvragen

De geïnterviewden worden in de gelegenheid gesteld aanvullende informatie, opmerkingen en/of aanbevelingen voor het onderzoek te geven.

- Zijn er nog aanvullende opmerkingen van uw kant met betrekking tot het interview of het onderzoek?
    - Dit type interviews is eigenlijk niet via videobellen uit te voeren vanwege het diepgaande karakter van deze onderzoeken.

8.2. Afsluitende opmerkingen

De geïnterviewde wordt bedankt voor zijn medewerking. Men wordt, indien gewenst, op de hoogte gehouden van de resultaten van het onderzoek. Tevens zal het verslag ter goedkeuring worden toegezonden voor deze verwerkt wordt in het onderzoek.

Bijlage G. Coderingsmatrix

Separaat bestand, onderstaande dient ter visualisatie.

Transscript Nr	Page	Textual Data	Categorie	Niveau	Open Coderen	Axiaal Coderen	Coder	Date
1	4	digitalisatie verondersteld dat een onderneming op zijn minst een minimale afhankelijkheid heeft van IT	Algemeen	Algemeen	ALG afhankelijkheid van IT	afhankelijkheid	Ben Slaager	5-jun-20
2	1	Kleine en middelgrote ondernemers zijn veelal te afhankelijk van hun leveranciers en moeten voldoen aan de eisen en manieren van deze grotere partijen.	Algemeen	Algemeen	ALG afhankelijk van anderen	afhankelijkheid	Ben Slaager	16-jun-20
2	1	Daarbij komt dat er ook teveel vertrouwen is in de security van deze grotere service providers en dat het vaak schort aan het hebben van goede SLA's	Algemeen	Algemeen	ALG afhankelijk van anderen	afhankelijkheid	Ben Slaager	16-jun-20
2	4	De tendens is dat er bij ondernemingen een steeds grotere afhankelijkheid van Cloud en SAAS diensten komt. Dit zorgt voor een valse mate van vertrouwen, eigenaarschap van risico's wordt steeds minder duidelijk.	Algemeen	Algemeen	ALG hoge afhankelijkheid van leveranciers	afhankelijkheid	Ben Slaager	16-jun-20
1	3	veelvoud van niet correct geïmplementeerde IT-middelen aanwezig is bij deze ondernemingen	Algemeen	Algemeen	ALG complexe IT architectuur	complexiteit	Ben Slaager	5-jun-20
1	3	niet correct geïmplementeerde IT-middelen	Algemeen	Algemeen	ALG misconfiguratie	complexiteit	Ben Slaager	5-jun-20
2	1	SAAS zorgt op zichzelf voor een heel nieuw scala aan security problemen en uitdagingen	Algemeen	Algemeen	ALG nieuwe risico's door nieuwe diensten	complexiteit	Ben Slaager	16-jun-20
2	1	steeds meer connectiviteit en bestaat dus het probleem dat ook alle data online staat en mogelijk voor kwaadwillende te benaderen is.	Algemeen	Algemeen	ALG nieuwe risico's	complexiteit	Ben Slaager	16-jun-20
3	1	Het is een zeer breed begrip en omvat alle risico's en maatregelen die voor kunnen komen met betrekking tot informatiesystemen. Vooral ook op het moment dat deze enigerwijs een koppeling hebben met internet	Algemeen	Algemeen	ALG koppelingen brengen nieuwe risico's met zich mee	complexiteit	Ben Slaager	16-jun-20
6	3	- Als de niveaus van de verschillende volwassenheidsmaatstaven niet gelijk lopen, loop je per definitie risico. De niveaus moeten in balans zijn, op zich zelf zeggen ze niet zo veel, maar in verbinding met elkaar wel.	Algemeen	Algemeen	ALG ongelijklopen van niveaus	complexiteit	Ben Slaager	16-jun-20
1	1	verdediging van digitale systemen, dus ook de Human-Machine interface.	Algemeen	Algemeen	ALG begrip cyber security	cyber security niveau	Ben Slaager	5-jun-20
1	1	90% van de MKB'ers en kleine ondernemers is niet Cyber secure.	Algemeen	Algemeen	ALG security niveau MKB	cyber security niveau	Ben Slaager	5-jun-20
2	1	Absoluut niet veilig, alleen worden de kleinere ondernemingen vooralsnog niet specifiek getarget. Ze worden wel meer en meer geraakt door willekeurige aanvallen zoals Ransomware	Algemeen	Algemeen	ALG security niveau MKB	cyber security niveau	Ben Slaager	16-jun-20
4	3	Als je aan de uiterste kanten zitten van de volwassenheidsschalen dan loop je voornamelijk business risico's, cyber risico's zitten meer in de tussenliggende niveaus.	Algemeen	Algemeen	ALG glijdende schaal van risico's	cyber security niveau	Ben Slaager	16-jun-20
4	3	- Als je aan de uiterste kanten zitten van de volwassenheidsschalen dan loop je voornamelijk business risico's, cyber risico's zitten meer in de tussenliggende niveaus.	Algemeen	Algemeen	ALG cyber risico's voornamelijk in tussenliggende niveau's	cyber security niveau	Ben Slaager	16-jun-20
5	1	Cybersecurity is een middel en geen doel, het zorgt ervoor dat handelingsvrijheid blijft bestaan.	Algemeen	Algemeen	ALG security is doel, geen middel	cyber security niveau	Ben Slaager	16-jun-20
5	1	We zitten niet meer in de volledige beginfase, maar we zitten ook zeker nog niet op een professioneel niveau.	Algemeen	Algemeen	ALG MKB cybersecurity zit in een lift, nog lang niet waar nodig	cyber security niveau	Ben Slaager	16-jun-20
5	3	- Als je aan de uiterste kanten zitten van de volwassenheidsschalen dan loop je voornamelijk business risico's, cyber risico's zitten meer in de tussenliggende niveaus.	Algemeen	Algemeen	ALG cyber risico's voornamelijk in midden niveaus	cyber security niveau	Ben Slaager	16-jun-20

Bijlage H. Validatie vragenlijst respondenten

Beste Respondent,

Naar aanleiding van het afgenomen interview zou ik u kort nog een aantal vragen willen stellen aan de hand van deze questionnaire. Met behulp van de interviews die ik de afgelopen maanden heb afgenomen (waaronder die van u) ben ik tot een verbetering van het toentertijd voorgelegde model gekomen. Daarnaast heb ik met behulp van uw antwoorden een invulling kunnen geven aan de risico's voor een MKB ondernemer afhankelijk van het volwassenheidsniveau in de categorieën: proces, digitalisatie en genomen cyberweerbaarheidsmaatregelen.

Allereerst het verbeterde model, waarbij (op basis van de ontvangen feedback) gekozen is om het aantal niveaus terug te brengen van vijf tot drie en aansluitend een drietal vragen.

Mate van genomen cyberweerbaarheidsmaatregelen

Mate van volwassenheid procesinrichting en digitalisatie

Volwassenheidsniveau	Initial	Basic t/m Efficiency	Optimizing
Ad-Hoc	• Bedrijfscontinuïteit • Geen indicatoren / Detectie • Wettelijke aansprakelijkheid • Makkelijk doelwit / kwetsbaar • Onnodige kosten op termijn • Geen herstel	• De medewerker • Onnodige kosten • Geen indicatie op incidenten • Weerstand tegen maatregelen • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Bedrijfscontinuïteit in gevaar • Efficiëntie beperkingen • Mens als risico factor • Gebruiksvriendelijkheid neemt af • Schijnveiligheid • Zeer hoge kosten • Cybermoeheid
Engaged t/m Managed	• Afhankelijkheid van anderen stijgt • Connecties zijn onbekend • Scheefgroei • Toenemende complexiteit • Introductie van nieuwe risico's • Kennis als knelpunt • Geen herstel • Hoge kwetsbaarheid • Juridisch aansprakelijk • IT als grootste risico	• Afhankelijkheid van anderen stijgt • Scheefgroei • Toenemende complexiteit • Kennis als knelpunt • Weerstand • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Toenemende complexiteit • Kennis als knelpunt • Afhankelijkheden stijgen • Gebruiksvriendelijkheid neemt af • Schijnveiligheid • Zeer hoge kosten • Cybermoeheid
Optimized	• Afhankelijkheid van externen • Verkeerde doelstellingen • Hoge overhead kosten • Schijnveiligheid • Verminderde flexibiliteit • Hoge mate van complexiteit • SPOF • Nieuwe risico's worden geïntroduceerd • Hoge kwetsbaarheid • Juridisch aansprakelijk • IT als grootste risico	• Afhankelijkheid van externen • Verkeerde doelstellingen • Hoge overhead kosten • Verminderde flexibiliteit • Hoge mate van complexiteit • SPOF • Nieuwe risico's worden geïntroduceerd • Weerstand • Efficiëntie beperkingen • Vatbaar voor complexere aanvallen	• Afhankelijkheid van externen • Verkeerde doelstellingen • Hoge overhead kosten • Schijnveiligheid • Hoge mate van complexiteit • Cybermoeheid • Hoge mate van complexiteit

1. Wat vind u zo op het eerste oogopslag van het gevulde model?

2. Detailvragen:

    2a. Als u de kennis die u heeft van bestaande MKB ondernemers projecteerd op dit model, herkent u zich dan in de beschreven risico's ten opzichte van de volwassenheidsniveaus?

    2b. Als men verder investeert in cyberweerbaarheidsmaatregelen (men gaat 1 kolom naar rechts), herkent u dan de resterende benoemde risico's?

    2c. Als men verder investeert in digitalisering en procesvolwassenheid (men gaat 1 rij naar beneden), herkent u dan de resterende benoemde risico's?

3. Heeft u nog aanvullingen op het model?

Hartelijk dank voor uw reactie,

B.F.L. Slaager

Bijlage I. Uitkomst validatie respondenten

1. Wat vind u zo op het eerste oogopslag van het gevulde model?
- Oogt overzichtelijk, duidelijke gecategoriseerd en “trapsgewijs”.
- Lees prettig door verschillende kleurlijnen/kleuronderscheid/Wellicht drie kleuren van maken, mocht je nog een prioriteit/impact aan willen geven.
- Het model vind ik vrij druk gevuld en lijkt op eerste oog opslag alleen maar negatief te zijn. Na het beter te bestuderen geeft het een duidelijk beeld van de risico's naar gelang de voortgang van de organisatie.
- Prettig dat de tussenliggende maturity levels samengenomen zijn. Dit kwam in het interview al naar voren en lijkt mij voldoende abstractieniveau voor mkb-bedrijven.
- Risico’s voor MKB’er zijn overzichtelijk weergeven per vlak. Ook een duidelijke verdeling in de verschillende volwassenheidsniveau’s. Zonder inhoudelijke voorkennis van het model, is het voor een “redelijk geinformeerde derde” naar mening goed leesbaar. Moest alleen SPOF even opzoeken.
- Voldoende diepgang en progressie tussen de stappen. Lijkt een compleet beeld te geven.

2a. Als u de kennis die u heeft van bestaande MKB ondernemers projecteert op dit model, herkent u zich dan in de beschreven risico’s ten opzichte van de volwassenheidsniveaus?
- Voor zeer groot deel wel. Ik ben geen absolute MKB cyber expert, maar kan nagenoeg alle risico’s onderbouwd herleiden naar bestaande MKB ondernemers en de gehanteerde variabelen (x- en y-as)
- Wij kennen als organisatie met name bedrijven die aan het begin van hun digitale maturity staan. Daar herken ik zeker een aantal risico’s, zoals bedrijfscontinuiteit (bijvoorbeeld bij een ransomware-aanval) of het zijn van een gemakkelijk doelwit (bijvoorbeeld omdat er geen updates uitgevoerd worden).
- Ja, ik denk dat zeker risico’s zijn die bij MKB ondernemers aanwezig zijn.

2b. Als men verder investeert in cyberweerbaarheidsmaatregelen (men gaat 1 kolom naar rechts), herkent u dan de resterende benoemde risico's?
- Ik herken de resterende risico’s. Afhankelijk van de risk-appetite / risicobereidheid van de organisatie dienen ook die risico’s behandeld te worden (mitigeren, negeren, uitsluiten etc..)
- Ja en nee, de medewerker zou ook een risico kunnen zijn in level 1. Net als ‘mens als risico factor’ in level 3. Weerstand tegen maatregelen daarentegen komt (natuurlijk?) pas voor als er daadwerkelijk maatregelen genomen gaan worden bij de hogere maturity niveaus.
- Ja, toename complexiteit in cybermaatregelen kan weer zorgen voor afname gebruikersvriendelijkheid. Dus ik herken de verandering in risico indien naar rechts in het model wordt gegaan.

2c. Als men verder investeert in digitalisering en procesvolwassenheid (men gaat 1 rij naar beneden), herkent u dan de resterende benoemde risico's?
- Ja. Lijken mij logische restrisico’s (of juist nieuwe risico’s)
- SPOF is single point of failure? Zo ja, waarom bij een hoge mate van digitalisering? Naar mijn idee heb de dan juist geen SPOF meer. Afname van flexibiliteit lijkt mij inderdaad een risico bij een hogere mate van procesvolwassenheid, net zoals de afhankelijkheid van externen.
- Ik herken de benoemde risico. Vind deze beweging eerlijk gezegd lastiger te herkennen dan de beweging naar rechts. Maar ik herken de risico’s wel. Alleen verminderde flexibiliteit vind ik lastig te interpreteren. Procesoptimalisatie kan ook weer voor toename flexibilteit met zich meebrengen. Voor de rest geen opmerkingen.

3. Heeft u nog aanvullingen op het model?

- Let op mixen van NLD en ENG
- Misschien net iets te veel bullits
- Ik zou “mate van genomen cyberweerbaarheidsmaatregelen + pijltje aan de onderkant i.p.v. bovenkant zetten. Vervolgens titel bovenaan plaatsen van het model
- Ik zou het model overzichtelijker maken zodat er in eerste opslag duidelijkheid is plaatjes ipv teksten etc.
- Er lijkt wel sprake te zijn van verschillende detailniveaus van genoemde risico’s. Bijvoorbeeld ‘de medewerker’ <-> ‘Geen herstel’. Hoe zou je het categoriseren? Wellicht eentje voor vervolgonderzoek
- Geen opmerkingen. Voor de MKB’er die van plan is om te gaan investeringen heel handig om te weten met welke risico’s rekening gehouden dient te worden (en daar weer mitigerende maatregelen voor te nemen).
- Bij Ad-Hoc ontbreekt in de linker kolom de juridische aansprakelijkheid. Je zou juist verwachten dat deze bij weinig/geen aandacht voor cyberweerbaarheid het hoogst is en dus juist in dit vakje opgenomen zou worden.